S. HRG. 118–110

REINING IN DOMINANT DIGITAL PLATFORMS: RESTORING COMPETITON TO OUR DIGITAL MARKETS

HEARING

BEFORE THE

SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MARCH 7, 2023

Serial No. J–118–6

Printed for the use of the Committee on the Judiciary

www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
53–536 PDF WASHINGTON : 2024

COMMITTEE ON THE JUDICIARY

RICHARD J. DURBIN, Illinois, *Chair*

DIANNE FEINSTEIN, California
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut
MAZIE K. HIRONO, Hawaii
CORY A. BOOKER, New Jersey
ALEX PADILLA, California
JON OSSOFF, Georgia
PETER WELCH, Vermont

LINDSEY O. GRAHAM, South Carolina, *Ranking Member*
CHARLES E. GRASSLEY, Iowa
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TED CRUZ, Texas
JOSH HAWLEY, Missouri
TOM COTTON, Arkansas
JOHN KENNEDY, Louisiana
THOM TILLIS, North Carolina
MARSHA BLACKBURN, Tennessee

JOSEPH ZOGBY, *Chief Counsel and Staff Director*
KATHERINE NIKAS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS

AMY KLOBUCHAR, Minnesota, *Chair*

SHELDON WHITEHOUSE, Rhode Island
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut
MAZIE K. HIRONO, Hawaii
CORY A. BOOKER, New Jersey
PETER WELCH, Vermont

MICHAEL S. LEE, Utah, *Ranking Member*
CHARLES E. GRASSLEY, Iowa
JOSH HAWLEY, Missouri
TOM COTTON, Arkansas
THOM TILLIS, North Carolina
MARSHA BLACKBURN, Tennessee

KEAGAN BUCHANAN, *Democratic Chief Counsel*
WENDY BAIG, *Republican Chief Counsel*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

REINING IN DOMINANT DIGITAL PLATFORMS: RESTORING COMPETITON TO OUR DIGITAL MARKETS

TUESDAY, MARCH 7, 2023

UNITED STATES SENATE,
SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST,
AND CONSUMER RIGHTS,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice at 3:07 p.m., in Room 216, Hart Senate Office Building, Hon. Amy Klobuchar, Chair of the Subcommittee, presiding.

Present: Senators Klobuchar [presiding], Whitehouse, Coons, Blumenthal, Hirono, Lee, Grassley, Hawley, and Tillis.

Also present: Chair Durbin and Senator Padilla.

OPENING STATEMENT OF HON. AMY KLOBUCHAR, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Chair KLOBUCHAR. Sorry we were a little late, but the good news is, we got both votes done. So we won't be running back and forth. I call to order this hearing of the Subcommittee on Competition Policy, Antitrust, and Consumer Rights on "Reining in Dominant Digital Platforms: Restoring Competition to Our Digital Markets." I'd like to welcome our witnesses and thank Senator Lee and his staff for helping to plan this hearing.

We all know that a few dominant online platforms have the power to control whether and how businesses can access customers and markets online. These dominant platforms often abuse this power to preference their own products in a way that stifles competition and innovation.

Last Congress, between the House and the Senate, over 150 hearings on the tech issues were held. Let me say that again—one, I don't mean to not make you guys feel special—but, 150 hearings were held, and we did make progress.

In addition to the House report that Representative Cicilline and Representative Ken Buck, as well as the Chairs over in the House put out, we passed some bills.

The Senate Judiciary Committee, as you know, passed out the bill on changing the merger fees that Senator Grassley and I had, as well as the bill that Senator Lee and I had, that Senator Lee led on venues.

Both bills passed at the end of last year as a part of the year-end budget, and Senator Lee and I worked together. And I believe

those are very important pieces of legislation for assisting those at the State and Federal level that are going after these cases.

The Senate Judiciary Committee also reported the bipartisan American Innovation and Choice Online Act to the Senate floor, making it the first tech competition bill voted out of this Committee since the dawn of the internet. This isn't just about the money for enforcement or about State efforts. This is actually about Federal efforts and the need to change the laws to fit the times.

A few weeks later, the Open App Markets Act, something led by Senator Blumenthal, and Blackburn, and myself, was also reported out on a strong bipartisan vote, but after an unprecedented lobbying effort by the dominant platforms—as in, I remember in August of last year, they'd spent more money on legislation, according to a Bloomberg report, than any other entities, industries. Even more than Pharma had at that point.

I don't have updated numbers, but I know that nearly, probably over $200 million was spent against this bill in States all over the country with ads that had nothing to do with each other, for red States and blue States, to show their dominance. These bills did not get a vote on the floor.

And let me give you some numbers. I just noted the millions of dollars in advertising against the bills—$90 million on lobbying over the previous 18 months. In just one week last May, one industry group spent $22 million on TV ads against the American Innovation and Choice Online Act.

I—particularly, I want to note for the companies—enjoyed the pop-up ads run in DC against me that said, "Amy Klobuchar"—and I love the way your lawyers insisted on putting in small letters, "could."—"Amy Klobuchar could destroy Amazon Prime." "Amy Klobuchar could"— in really small letters—"destroy Google Maps." They were well noted. Congratulations on your money spent.

These companies have only become more brazen since then with armies of lobbyists and lawyers. They are in every corner in this town, at every cocktail party, and all over this building. But it's easy to see why they don't want us to act. We would be happy to work with the companies on legislation, but they shut every single thing down. Why? Because they can.

Google has 90 percent market share in search engines. Apple controls 100 percent of app distribution for iPhones. Three out of every 4 social media users use Facebook or Instagram. Amazon accounted for about 40 percent of the entire U.S. e-commerce retail market last year. That's dominance under any way of looking at the antitrust laws, something that I know the Justice Department is looking into, as we speak.

So while many have said all the right things about fostering innovation, helping small businesses, and improving privacy, when it comes to actual action, we have done nothing in this Congress. With the exception of the funding—which I will say is incredibly important—and the Venue bill, we have done nothing in terms of setting standards when it comes to tech.

Nothing out of the Congress on privacy. Nothing out of the Congress on updating the children's protection bills when it comes to the internet. Nothing on the Congress when it comes to dominance on the platforms and self-preferencing. Nothing out of the Congress

on AI. You can come to your own conclusions on why that has happened.

But I think you all know when you talk to parents who are trying to help their kids to do their homework, and not spend their whole day on social media, or be exposed to bad stuff. Or when you talk to small businesses, like those in the National—NFIB, the National Federation of Independent Businesses—which is not exactly known as a liberal group, that has endorsed the bill that we are in part talking about today—I think you then understand what's going on in this country, and why we need some rules of the road, and why there has been bipartisan support for these bills.

I'm well aware of what's going on in the House, and Congressman Buck, who I spoke to this morning, his loss of his Committee post—which he did so well—and I'm well aware of some of the changes made to that Subcommittee that have made it harder and harder for us to proceed with these bills. We have to be honest about that. But to just close our eyes and do nothing and let another 2 years go by is a huge mistake.

And that's why we're having this hearing, and that's why we're moving ahead. While we fail to act, the dominant platforms use their control to suppress the competition and rake in billions at the expense of consumers.

If you don't want Meta to have your data and sell it to advertisers, tough luck, because you will have to avoid using Facebook, Instagram, WhatsApp, and Messenger.

If you don't want to use the Apple App Store, tough luck, because there is no other way to get your apps on the iPhone.

And if you're a small business that wants to use a local delivery service instead of Amazon's shipping system, tough luck, because they're two. Because it is virtually impossible to get to the top of Amazon's search listings unless you buy Amazon's shipping systems.

Small businesses are beholden to digital gatekeepers that can block access to their customers, take their data, and demote them in search rankings while copying their best ideas and bringing them to market on their own. That discourages businesses from innovating and deters investors from putting money into startups. They all know the game is rigged.

We know that other countries are taking action. They are leading the way in the Digital Age. I wish we were. I know Senator Hawley has some ideas on how he would like to proceed. I know Senator Lee has tons of ideas. But in fact, let's be honest, that's not happening right now.

The European Union enacted the Digital Markets Act, which puts regulatory restrictions on how the largest digital platforms can use their power. Australia is considering similar reforms to protect digital competition.

I'm glad they're doing this. It will give us good examples. It will show that the market is still vibrant even when they protect their consumers and they have the guts to pass something.

The UK is considering legislation to further empower its digital markets union. And South Korea enacted new rules to open up app markets.

If Congress does nothing, we abdicate America's leadership position on global competition policy. We let foreign laws become the global standard for regulating American digital businesses around the world.

And while the dominant digital platforms lobby against legislation in the United States, they are agreeing to the same commonsense rules in other countries.

That may be the biggest hypocrisy of all. It's okay to give small businesses some rights in Europe. It's okay to have help for consumers and protection for consumers in the UK or Australia. But here, where they are allegedly hometown companies, where they're supposed to be looking out for Americans, they fight it tooth and nail.

The good news is that there's still a bipartisan majority in both Chambers that is ready to take action. Bipartisan legislation with Senator Grassley and other Members of this Committee, the American Innovation and Choice Online Act, as well as Representatives Cicilline and Buck in the House, which establishes rules of the road for dominant digital platforms and prevents them from favoring their own products or services just because they own them.

These are targeted reforms to address anticompetitive behavior, level the playing field for businesses, and increase choice while driving down costs for consumers. And these reforms do it without compromising privacy or security.

That's why, as the Attorney General said last week, the Department of Justice, along with the Commerce Department, endorses the bill. The bill also, as I already noted, has strong support from the National Federation of Independent Businesses, Consumer Reports, the Main Street Alliance, and Consumer Federation of America, and many civil society groups across the political spectrum.

I also joined Senators Blumenthal and Blackburn to introduce the Open App Markets Act to give app developers more power to reach their customers without the control of app stores run by Apple and Google. And I am working with Senator Lee on this bill to improve competition and transparency in ad technology markets. We're going to be having another hearing to focus on that soon.

Here's the bottom line: We cannot afford to waste another 2 years getting nothing done; another 2 years for these monopolists to further entrench their power; another 2 years of unchecked anticompetitive self-preferencing; another 2 years of small businesses closing up shop; another 2 years of failing to protect American consumers; while the rest of the world moves forward.

And I am well aware that the content arguments are used, and they're very different. The arguments that are made to the left from the right. One day I hope to publish the sentences that said that the companies give to the right and what they give to the left. And at some point, we know that they're the same because they're designed for one thing, and that is to stop these bills and maintain their dominant position.

I know eventually we're going to get this done, even if it means all these other countries went before us, and there'll be pressure for them to agree to it in America. Eventually, we will. But for the good of the people of this country, I hope it is sooner rather than

later. I look forward to continuing to work with colleagues on both sides of the aisle. And with that, I turn it over to Senator Lee.

OPENING STATEMENT OF HON. MICHAEL S. LEE, A U.S. SENATOR FROM THE STATE OF UTAH

Senator LEE. Thanks so much, Madam Chair. If it seems like we've had this hearing several times before, well, it's because we have. But it's also because finding a way to rein in the pernicious influence of Big Tech remains one of the most pressing public policy concerns of our time.

These aren't the first monopolies, by any means, that America has endured, and has had to figure out how to deal with. We've dealt with them before, but never before have we seen just a handful of trillion-dollar corporate bureaucracies exercising such pervasive control over how we stay in touch with friends and loved ones, how we shop to provide for our families, obtain news and other information, exercise our First Amendment rights, influence public debate, and even how we turn on our air conditioning, and lock or unlock our doors.

All of that is on top of the fact that they're doing stuff to our kids that many of us find very disconcerting. Big Tech's business plans are built on an addiction business model, and our children are uniquely vulnerable to fuel their growth and their expansion as attractive targets for those businesses.

What's sold as fun and as a matter of convenience seems to, more often, end up as a gateway to pornography and to Chinese propaganda. But for them, a click is a click. Yet, while Big Tech profits have grown significantly, so have teenage anxiety, depression, and suicide rates. These companies don't just track where we go, what we say, what we buy, who we talk to, what we read. They actively influence, and direct nearly every facet of our lives, to ensure that our patterns of behavior remain what's most profitable for them.

Not content to stifle competition in their respective commercial markets, Big Tech increasingly works to kill competition in the marketplace of ideas. Woke ideology is seeped from universities to the boardroom, and it's now being foisted upon consumers in the form of censorship and exclusion from the 21st-century public square. Even worse, we now know that these companies have been colluding with the Federal Government to do so. A gross violation of our constitutional rights.

It turns out Big Tech and Big Government share a lot in common, including their love for surveillance and censorship. They don't necessarily bring out the best in each other, and that's putting it mildly. So it's not surprising that so often when we see Big Tech tracking and censoring us, it turns out that Big Government was there, egging them along, facilitating it, perhaps requesting it, all along.

In the past, there was at least some consolation in the idea that market forces would eventually intervene, that changes in technology and new innovation would somehow disrupt incumbents and provide consumers with new choices. But today's monopolists, however, control much of the consumer technology and innovation themselves. And what they don't control, they actively endeavor to buy up before it can become a competitive threat that might actu-

ally risk displacing them or disrupting their control of the marketplace.

This is precisely why there's such a strong bipartisan support for the idea that we need to find ways to ensure that the same companies that began as innovative startups disrupting stagnant markets to improve the lives of consumers, don't end up as entrenched as the monopolists undermining competition at the expense of consumers and American society itself.

This is an incredibly important task, and one that I take very seriously, as someone who's long championed Congress' unique legislative prerogative and responsibility to make law. And neither the judiciary nor the executive branch can solve these problems alone. Congress must act.

At the same time, we also have a duty to ensure that the cure isn't something that turns out to be worse than the disease. As concerned as I am by the behavior of Big Tech, I'm equally concerned that some of the bills that have been introduced to solve one problem or another simply replace a corporate tyrant with a Government tyrant. They would replace a lack of competition with an excess of Government micromanagement by bureaucrats, trading one form of dysfunction for another.

Ironically, it's often this very kind of regulation that leads to consolidation in the first place, pushing firms to merge, thereby erecting barriers to entry, and protecting themselves from competition. Congress should prefer targeted, detailed legislative solutions to broad, vaguely defined grants of new authority to Federal agencies.

As I've said before, it's important that Congress solve the problems presented by Big Tech rather than broadly delegating the issue off to Federal bureaucrats and agencies subject to regulatory capture and unaccountable to voters. I remain particularly opposed to the idea of granting any new authority to the Federal Trade Commission.

Unfortunately, the radical agenda of the Biden FTC has made it even harder to find common ground in the fight against Big Tech. Even passing a bill to update the merger filing fee structure, something that should have been uncontroversial, was needlessly difficult and almost failed, simply because of the overreach and the incompetence of the FTC under the current administration.

I'm grateful to Senator Klobuchar for convening this hearing because we're here to discuss some really important issues, and for continuing to be a valuable legislative partner as we both work toward bipartisan solutions to shared challenges.

I look forward to our discussion today and a hearing later this month that we'll be having to discuss our AMERICA Act to tackle competition in digital advertising. Thank you, Madam Chair.

Chair KLOBUCHAR. Thank you, very much, Senator Lee. And now I want to introduce our witnesses.

Fiona Scott Morton is a professor of economics at the Yale School of Management, where she teaches competitive strategy and antitrust economics.

Chris Lewis is president and CEO of Public Knowledge, a nonprofit public interest group in digital competition.

Daniel Francis is an assistant professor of law at New York University.

Adam Candeub is the director of the IP, Information & Communications Law Program at Michigan State University.

And Amanda Lewis is a partner at Cuneo Gilbert & LaDuca, LLP where she specializes in antitrust and consumer protection.

If the witnesses could now please stand and raise your right hand.

[Witnesses are sworn in.]

Chair KLOBUCHAR. Thank you. You may be seated. I will now recognize the witnesses for 5 minutes of testimony each, starting with you, Professor Scott Morton. Thank you.

STATEMENT OF FIONA M. SCOTT MORTON, THEODORE NIERENBERG PROFESSOR OF ECONOMICS, YALE SCHOOL OF MANAGEMENT, NEW HAVEN, CONNECTICUT

Professor SCOTT MORTON. Thank you, Chair Klobuchar and Ranking Member Lee, for the invitation to testify today. I have only a few points to make.

The modern interpretation and application of U.S. antitrust laws has failed to preserve competition in today's digital platform markets. Relying on entrenched monopolists to innovate and create competition is foolhardy and unsupported by economic learning. The perfect antitrust law would be a great help, and I would firmly support that.

But my understanding is that such a law is not on the menu today, and will not be anytime soon. This means our choice is between the status quo and the bills we're here to discuss today.

Larger budgets for antitrust enforcement are also necessary, and I support those. But litigation is an expensive, uncertain, and slow method to stop the behaviors Congress, and many other jurisdictions, have identified as problematic.

Current antitrust enforcement actions against Big Tech also run up against the problem of what remedy to request should the Government prevail. How can agencies restore the lost competition? In the absence of prompt and effective remedies that create competition in platform markets, a good alternative is a set of rules that stimulates competition on dominant platforms. The apps, vendors, and other businesses that use these platforms are businesses that will not invest and invent unless they have a route to profitability.

AICOA is quite conservative in that it aims to restore competition to digital markets that are concentrated or monopolized. The bill is fit for purpose and makes actionable only those violations that injure competition. The deference generally given to affirmative defenses in our current system—an undue deference, in my opinion—very often indicates that the law is very unlikely to penalize reasonable actions and quality products.

The Protect Competition language in AICOA is new exactly because we know we have an antitrust enforcement problem. Using language drawn from the same ineffective jurisprudence we now use today would yield the same ineffective outcomes we have today, namely, insufficient protection of competition.

I expect it will take many years until we have a digital regulator, just as it took much human suffering before Congress chose to create regulators for industries like pharmaceuticals and railroads. Until we have such a regulator, the laws being proposed today are

the best route to immediate improvements for the welfare of consumers.

The pair of bills that we're discussing today reflect some of the content contained in the Digital Markets Act, which Senator Klobuchar referenced a few minutes ago and which will take effect in Europe in January 2024, less than 9 months away.

Let me give you a few examples of the requirements in that law.

Article 5, number 4 is anti-steering and an anti-gag rule. Gatekeeper shall allow business users to contract, communicate, promote, deliver various services bought elsewhere through the core platform. So this gives app developers much more freedom than they have today.

Article 5, item 7. Prohibition on tying a platform with an in-app payment system, that gets freed up.

Article 6, item 2. Prohibition of the use of nonpublic business user data to compete against the business users.

Article 6, item 4. An obligation to open operating systems to third-party apps and app stores. "The gatekeeper shall allow and technically enable the installation and effective use of third-party software applications or software application stores."

Article 6, number 5. "The gatekeeper shall not treat more favourably, in ranking and related indexing and crawling, services and products offered by the gatekeeper itself than similar services or products of a third party."

Article 6, item 7. Free interoperability. So free, no access charge, interoperability for business users, hardware, and software that is equivalent to the access enjoyed by the platform's own hardware and software.

As you can see from this limited selection, the DMA is much more detailed than the text of AICOA or OAMA, and does not include any efficiency defense. In particular, the DMA does not require that the regulator show that each instance of prohibited conduct harms competition. Instead, the rules were chosen to be those that, in the view of the European Parliament, would generally protect and increase competition. Platforms must be in compliance with these rules by 2024 in Europe.

What does this mean for the bills we're discussing today? Right now, companies that seek to compete against today's dominant platforms, or offer services through them, will have an enormous incentive to focus their efforts in Europe where they can bring new services, innovations, and lower prices to European consumers with these changes in the laws that give them more access, control, and innovative ability.

American businesses and consumers will be able to read about these innovations, but they will need to go and launch a product in Europe themselves or visit on vacation to experience those products.

The United States will miss out on opportunities to lead the world in tech sector innovation and experience the benefits that that innovation can deliver. Thank you.

[The prepared statement of Professor Scott Morton appears as a submission for the record.]

Chair KLOBUCHAR. Thank you, very, very much. Next up, Chris Lewis. Thank you.

STATEMENT OF CHRIS LEWIS, PRESIDENT AND CHIEF EXECUTIVE OFFICER, PUBLIC KNOWLEDGE, WASHINGTON, DC

Mr. LEWIS. Thank you, Chair Klobuchar, Ranking Member Lee, for the invitation to testify today. Public Knowledge is a nonprofit digital rights organization whose mission is to fight for an open internet, free expression, and affordable access to communications tools and creative works. And we see promoting robust competition online as a key part of that mission.

Tech users are increasingly feeling like they have no power over tech giants online and, at times, feel stuck with them. Big Tech companies are popular for the democratic speech they support, for the ease of purchasing products, and the communities that they foster. However, there is a distinct downside.

Consumers don't know or understand how they are being tracked or influenced. Small businesses must accept unfair treatment in order to access consumers through the digital platform that dominate the internet. Their products can be unfairly demoted in search results, their ability to communicate with their customers can be limited, and their competitively sensitive business information can be misused.

On social media, where so much of our modern political debate takes place, women, people of color, and other marginalized communities, face harassment that pushes us out of the conversation. Radicalization pipelines on social media have offline consequences.

Digital platforms are a distinct sector that need new laws and rules to address their power and protect users. Antitrust laws have an important role to play here, but existing antitrust law will not be sufficient.

Here's a four-part framework that we've come up with for how I think we can best address the variety of policy challenges posed by dominant digital platforms.

The first is the subject of this hearing. Competition. We need sector-specific, pro-competition legislation to empower consumers and business users by incentivizing market entry, and facilitating switching to new platforms.

Competition empowers customers to choose the option that is best for them. In many markets, that's the best price. But in digital platforms, where the price is often $0, competition may happen along a variety of quality measures.

Consumers might prefer to see fewer ads, more relevant search results, more reliable information, perhaps filtering tools, or antiharassment tools, or even more, or less, content moderation.

The American Innovation and Choice Online Act, AICOA, and the Open App Markets Act, will make sure consumers are actually seeing the products that are best for them and not just products that are best for tech's bottom line.

By taking away some of the key tools that Big Tech uses to stifle competitors and potential competitors online, fair competition rules, like those found in AICOA and the Open App Market Act, will also encourage new innovation to enter the market, since they'll know that they can have a fair shot to actually reach customers.

Briefly, the other three parts of the framework are important as policymakers address sustainable solutions to meet consumers' needs.

Part two is the importance of transparency so that consumers and business users can make informed choices. Transparency and due process practices, paired with interoperability requirements, can build trust and empower users when it comes to content moderation.

Third, we need consumer protection laws and rules to address platform harms that won't be improved by competition. The first, and most important, of these will be a comprehensive privacy bill, like the ADPPA, which we support. Everyone deserves to have their privacy respected.

Last, these responsibilities should be housed in a new agency, an expert digital regulator. This regulator would work together with antitrust enforcers, not in lieu of antitrust enforcement. It would have competition, privacy, and other consumer protection authorities. It could also address content moderation concerns through transparency and due process requirements. And it could help carefully craft the future of algorithmic oversight and accountability.

Given the bipartisan work of Congress over the past few years, we believe this framework can build a foundation for a better internet in the future. I know folks may disagree on some of the details of these legislative proposals, but we are happy to work with you, and other stakeholders, to find workable solutions. So thank you for inviting us here today, and I look forward to your questions.

[The prepared statement of Mr. Lewis appears as a submission for the record.]

Chair KLOBUCHAR. Thank you, very much. Next up, Professor Francis.

STATEMENT OF DANIEL FRANCIS, ASSISTANT PROFESSOR OF LAW, NEW YORK UNIVERSITY, NEW YORK, NEW YORK

Professor FRANCIS. Chair Klobuchar, Ranking Member Lee, Members of the Subcommittee, thanks for inviting me today. I'm a former Federal antitrust enforcer, and I strongly support the Subcommittee's focus on tech monopoly.

Our digital markets are not competitive enough. Antitrust enforcement needs more money, building on the recent wonderful successes, and it needs updated statutes so that we can stop anticompetitive acquisitions and exclusionary practices in tech and other markets. And I would support platform rules that were targeted at specific practices that used market power in anticompetitive ways to harm consumers. But I don't recommend enacting either of these bills under discussion today.

First, I don't support AICOA because I read it as telling platforms to do less for consumers and more for other businesses, some of which are going to turn out to be bad or harmful.

Point one: AICOA makes it presumptively illegal to do many things that benefit consumers. Integrating functions like putting map information in search results, pre-installing apps like mail or maps on a phone, bundling services like music or movies in with Amazon Prime—those things shouldn't be even presumptively illegal.

Point two: AICOA is going to discourage platforms from protecting users. There are plenty of bad actors, malicious apps, and junk out there on the internet. And today, platforms protect users by restricting access.

But under AICOA, those access restrictions are going to mean a threat of serious hassle, at best—complaints, lengthy investigations, the threat of huge penalties and injunctions, and even the forfeiture of personal compensation by executives. And that threat's going to be bigger because so much of AICOA is vague.

So, it's going to be much less attractive for platforms to protect users than it is today. Now, that's going to mean that some good actors will get access to platforms and users, and that will be good.

But more bad actors are going to get access, too. They're going to be pre-installed on devices, they're going to be available in app stores, they're going to be available to choose as a default, given access to cameras, and microphones, and GPS information. And I think that's a much bigger harm.

Point three: The affirmative defenses are much too weak. There's no defense here on the ground that what was restricted was just a bad product, or it was full of spam, or intrusive advertising. Or full of false, or objectionable, or sexually explicit content. Or just too expensive to integrate.

There is a product improvement defense, but it's only limited to core functions. If you improve a noncore function, it doesn't apply. And the defense doesn't apply at all if what you're doing could be done in a less discriminatory way, even if doing it that way would be unprofitable.

And relying on the affirmative defense at all means spending time and money to prove it, risking penalties and injunctions, and even the loss of your own salary if a court ends up disagreeing. So, I think it's going to be a paper shield in practice.

Point four: Crucially, the bill doesn't define the central concept of harm to competition. It could mean either an antitrust-style consumer welfare test or injury to rivals. It can't possibly be both. And if it's the latter, then it's no limit at all. And if it's the former, which would allay a lot of my concerns, it must say so explicitly.

Point five, and finally, AICOA is going to inject a ton of confusion into tech markets. It's full of terms and concepts that are new, important, broad, and undefined. And it's going to drown in complaints the very same agencies that today barely have the resources to cover their antitrust docket. I think that's the last thing they need. And I can imagine State attorneys general taking really different views in perfectly good faith about how AICOA should work, including how content moderation fits under Sections 3(a)(3) and 3(a)(9) of the bill.

Very briefly on the app store bill, I think it's a much more promising basis for discussion. I would support rules for app stores that have significant market power. A ban on app price MFNs, a narrow ban on the competitive use of some data that preserve their right to use their own data and to buy it from developers, and I'd support a mandatory disclosure requirement when paid advertising leads to a search ranking boost.

But forcing third-party app stores into digital ecosystem threatens real harm. The whole cybersecurity world, from the NSA, and

the FBI, to the FTC, tell consumers and users to stay away from third-party app stores. I think the last thing we should do is lift those up.

I don't think, even though I've been negative in my presentation, that there are any easy answers here. Just really hard tradeoffs and best guesses about what consequences are going to be. My instinct is that we do a lot better supporting and investing in the antitrust system that we've got, which so badly needs support. I think that's a better deal all around. Thanks for having me today, and I look forward to your questions.

[The prepared statement of Professor Francis appears as a submission for the record.]

Chair KLOBUCHAR. Thank you. Next up, Professor Candeub.

STATEMENT OF ADAM CANDEUB, PROFESSOR OF LAW, MICHIGAN STATE UNIVERSITY, EAST LANSING, MICHIGAN

Professor CANDEUB. Madam Chair, Ranking Member Lee, and Senators, thank you for the chance to speak to you today. Big Tech's market power undermines our Nation's culture of vibrant——

Chair KLOBUCHAR. Sorry. You have to turn your microphone on, Adam.

Professor CANDEUB. Big Tech's market power undermines our Nation's culture of vibrant democratic deliberation. Elon Musk's Twitter files demonstrated that Big Tech has indeed limited particular groups, including dissenters, from important Government policies from full participation in national political discussions. This power to exclude threatens all Americans. Power to silence one group of Americans will be used sooner or later to silence another.

Consider Parler. Beginning in 2021, the social media company, which differentiated itself from competitors by its free speech policies, was the most downloaded app on the Apple Play Store. But then, on seemingly pretextual grounds, Apple removed Parler from the App Store, and soon after, Google removed it from the Play Store. Then Amazon Web terminated its hosting agreement. The Parler app was quite literally taken down, only returning online months later. It never recovered its growth momentum. And this problem, the problem of Big Tech, stems from its market power, and not simply Silicon Valley's moral outlook that may differ from that of most Americans.

As price givers, they dominate certain online business niches. And internet platforms can decrease service quality, silence viewpoints, perspectives without experiencing revenue loss. Competitive markets do not discipline their behavior.

Antitrust addresses market power and presents to many, including myself, a dilemma. I stand on the side of markets and economic freedom, but at the same time cannot close my eyes to Big Tech's deleterious effects on the institutional resilience of our democracy, free speech, children's health and development, as well as, quite possibly, on economic innovation and growth.

Antitrust has long recognized that special rules apply when dealing with market power deployed to stifle free speech and free expression. The Supreme Court, in *Associated Press v. United States*,

makes that point, and I quote, "The First Amendment, far from providing an argument against the application of the Sherman Act, here provides powerful reasons to the contrary. That amendment rests on the assumption that the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public." So from my perspective, I ask whether the Open App Markets Act and AICOA further a freer country, a stronger democracy, as well as a more vital and innovative online economy.

The Open App Markets is a solid attempt to combat the power of the large app distributors, but can be strengthened. As written, it's not clear that it would solve the Parler problem. There is no unreasonable discrimination provision that prohibits arbitrary de-platforming. Further, Section 4 exceptions allow platforms to exclude or de-platform apps to further digital safety.

As a law professor who specializes in communications law, I confess I never heard the term until I read it in the bill. What does digital safety mean? Don't text and drive? Don't charge your iPhone while using it in the bathtub? Alas, no.

Digital safety is a concept pushed, and likely coined, by the World Economic Forum and its Global Coalition on Digital Safety. The WEF defines digital unsafe content as, I quote, "lawful, but awful." As the Twitter files show, employees of the major platforms have notions of what constitutes awful, which probably do not align with what the Davos crowd considers awful, and which are probably quite contrary to American traditions of free expression.

As for AICOA, its Sponsors should be congratulated for reforwarding the issue of restoring competition in digital markets. I do have a few reservations. AICOA may simply be ineffective at promoting free speech. With no private cause of action, it is a very big stick, really a club, that DOJ, the FTC, and the State attorney generals can use to hit Big Tech.

As was observed in the opening comments, Government power for Big Tech often can have a bad effect on free speech. AICOA, with its open-ended terms, and discretionary and exclusive Government enforcement, adds to the available pressure Government can employ on the major internet platforms to silence Government's critics. I welcome the Committee's questions. Thank you.

[The prepared statement of Professor Candeub appears as a submission for the record.]

Chair KLOBUCHAR. Thank you, very much. Ms. Amanda Lewis, thank you for being here.

STATEMENT OF AMANDA LEWIS, PARTNER, CUNEO GILBERT & LADUCA, LLP, WASHINGTON, DC

Ms. LEWIS. Chairwoman Klobuchar and Ranking Member Lee, thank you for the invitation to testify. I am here in my personal capacity and not on behalf of any client.

Last Congress showed strong bipartisan support for antitrust reform, especially for bills that would curb Big Tech's and Big Pharma's monopoly power. There is a lot of common ground here. This Committee advanced AICOA and the Open App Markets Act on a bipartisan basis. You deserve credit for doing so.

Enforcers, as well as private plaintiffs, are currently seeking relief in court to address some of the gatekeeper platforms anticompetitive conduct. But the unique challenges of digital markets, plus the time and resource-intensive nature of litigation, make this an inefficient, and also possibly ineffective, tool for the job.

Under current law, the deck is stacked in favor of the platforms. And that is why Congress should pass legislation to rein in the dominant digital platforms and restore competition to our digital markets.

AICOA is a comprehensive and well-thought-out bill. It draws support from a long list of consumer groups, businesses, and labor unions. It counts both NFIB and the Teamsters as strong supporters. An example will help identify just a few concrete benefits of the bill. AICOA would prohibit Amazon from tying, which forces third-party sellers to pay enormous fees to Amazon for services that they don't actually want to buy.

By prohibiting this conduct, AICOA will restore dignity and autonomy to businesses that have no choice but to rely on Amazon. Independent businesses will cease to be puppets with Amazon pulling the strings.

Consumers will also benefit when sellers are no longer forced to pay junk fees to Amazon that effectively add up to a 50 percent commission on every sale. Sellers will undoubtedly pass those savings on to consumers. And this is just one example of many of the benefits of AICOA.

The Open App Markets Act is much narrower. It's focused on the mobile app ecosystem. If OAMA is passed, consumers will see immediate savings, as well, when Apple can no longer force a 30 percent commission on developers for payment services that should cost a fraction of that. OAMA would also force Apple to give consumers the same freedoms that they enjoy on their desktop and laptop computers, the freedom to download the software and services of their choosing. This would put the power back where it belongs: not in the hands of the dominant platforms but in the hands of consumers.

Finally, OAMA will restore the incentive to innovate for app developers. When innovators are no longer afraid that Apple will effectively steal their ideas and hard-won customers, they will take more risks and invest in new ideas. An increased sense of security will encourage the investment of capital in the innovation economy.

After this Committee's hard work to study the problems and the solutions, these bills are ready to become law. I urge Congress to move quickly to pass both AICOA and OAMA. Thank you.

[The prepared statement of Ms. Lewis appears as a submission for the record.]

Chair KLOBUCHAR. Thank you, very much, to our witnesses.

I'll get started here. We have a number of Senators with us. I'll start with you, Professor Scott Morton. I was interested to see already the 2,800 lawyers and lobbyists for the companies are now claiming that one of my points was that we should cede regulation to—that I said, we should cede regulation to Europe, and to Australia, and to South Korea. They're already at it.

I think you know what I said, which was, that we should take the lead. We in America, who believe in competition, should take

the lead. And that we have some good examples out there, but we shouldn't let them take the lead. So, I just thought for those of you tweeting that out, you might be interested to note that that was a lie.

Professor Scott Morton, could you please talk about, and kind of refute, some of the points that Professor Francis made when it comes to the bill, and how the bill is all about capitalism and competition? And as you know, throughout history, that has been a counterweight to monopolists.

Professor SCOTT MORTON. Thank you, Senator Klobuchar. I think the parade of horribles that was listed by Professor Francis really can't happen if there's a requirement to find injury to competition. Today's courts are actually really happy to find behaviors that economists would identify as harmful to competition, to be fine.

The problem we have is actually excessive deference to that kind of an argument. And I think, therefore, it's natural we would have some of that here despite the beefed-up language. So the notion that courts will suddenly eliminate quality products because they have to evaluate a harm to competition is, I think, misplaced.

And the kind of self-preferencing that the bill is worried about can be harmful. This is known. It's not an imaginary thing.

And Professor Francis has himself written that self-preferencing isn't captured by the antitrust laws—the current antitrust laws. So what kind of self-preferencing would we worry about? What kind would be harmful? The kind that harms competition.

So, again, we're returning to familiar economic concepts. This is all stuff that we know from the literature. And the fact that new words are being used in this legislation is exactly to ensure that we get a new outcome. We can't use the same terminology and imagine that courts won't understand it the way they always have. So, to get a different outcome, we have to use a new word and say, look, we're worried about harm to competition.

In terms of innovation, I think, as I said in my opening remarks, the entrenched monopolists that we have right now are not—should not be relied on to generate innovation. That's not what a monopolist does. It's safe. It doesn't have to run fast to innovate. Where we're seeing quite a lot of innovation is actually on these platforms now. So the apps themselves competing with each other and trying to innovate and indeed someday replace the platform. That gets limited without protections.

Chair KLOBUCHAR. Okay, thank you. Ms. Lewis—we have two Lewises. So I'll start with you, Ms. Lewis. This Committee found your testimony very interesting and compelling about the small businesses. And I think you know we have previously heard from them. Their group, the NFIB, is strongly in support of this bill. And many of them have told us they're afraid to come forward individually because they're afraid of retaliation by the platforms. And we've seen this before because they can go out of business if they're retaliated against.

You work with companies who are stuck in this position. How would the American Innovation and Choice Online Act help them?

Ms. LEWIS. Thank you, Senator Klobuchar. The fear of retaliation is significant and really overwhelming for many market participants. It is something that I encountered during the House Ju-

diciary Committee digital markets investigation and have continued to experience in private practice.

It's one of the reasons why I co-founded the Responsible Online Commerce Coalition: because small businesses, like Amazon third-party sellers, are terrified—terrified of the degree to which Amazon has complete control over their economic livelihood and the power to essentially eliminate it overnight.

The AICOA very helpfully explicitly prohibits retaliation when businesses of all sizes, and individuals, too, I believe, raise concerns about these platforms anticompetitive conduct. And that is a key provision, and I applaud you for that.

Chair KLOBUCHAR. Thank you. Last question, Mr. Lewis. How do you think the bill will affect the strength and competitiveness of U.S. tech companies?

Mr. LEWIS. Senator, I think it will affect it directly. Too many small companies rely on these platforms for access to consumers. And so it's important that they have the ability to reach consumers without having to ask for permission. It's important that they feel free to innovate without fear of their business data being manipulated by the dominant digital platforms.

So, most of the folks that we talked to, folks that were studied in the House antitrust investigation, folks who don't always want to come forward and share their fears, will say privately that it's important that they have the ability to compete. That they feel restricted by the practices of the dominant digital platforms.

Chair KLOBUCHAR. Okay.

Mr. LEWIS. And I feel like AICOA specifically targets the harms that we saw studied in the House Antitrust Subcommittee.

Chair KLOBUCHAR. Thank you, very much. And I just think it's really important to note as Ms. Lewis was talking about the momentum for the bill, we have had major breakthroughs, including the NFIB endorsement, since this started. And these things take a long time. And we—the more and more small businesses that, I think, that these platforms took for granted that are coming out and talking about what's happening, and including medium-sized businesses, and the like. I think it's really important that we note that kind of momentum that we've had, in terms of a change of the support that we're getting for this bill, as more people understand what's really going on, which—in this ecosystem, and what's going on around the world. Senator Lee.

Senator LEE. Thank you.

Professor Francis, I'd like to start with you, if that's okay. I share many of the concerns that have been expressed by colleagues that self-preferencing by dominant digital platforms may, in some circumstances, harm competition. But I'm also concerned that the broad, vague language used in AICOA could actually prohibit conduct—some conduct that's procompetitive as well. Do you share this concern? And if so, can you elaborate?

Professor FRANCIS. Very much, Senator. So, the bill makes central, as a limiting principle, the concept of harm to competition. And that's going to mean one of two things. Either antitrust-style consumer welfare, or injury to rivals or competitors. And the bill inexplicably leaves that vacant.

Professor Scott Morton is exactly right. Antitrust does have a concept of competitive harm. Not exactly the statutory language that AICOA has chosen, but consumer welfare. The use of market power to make consumers, or trading partners, or workers, worse off overall. It's a harm requirement.

And if AICOA said that, then my written testimony would have been much shorter and my concerns would have been allayed. But it doesn't. It could just mean injury to competitors, and that's what creates these terrible dangers.

Senator LEE. Thank you, that's helpful.

Professor Candeub, as I've mentioned, censorship isn't necessarily itself an antitrust problem. But market power can certainly enable, and in some cases markedly exacerbate, censorship.

I think that we need to deal with the censorship issue head-on, on its own terms. Which is why I'm preparing to introduce legislation that would prevent social media companies from acting as censor in private communications between one person and another, and would require them to be transparent and offer due process to their users when moderating public content while still allowing for the removal of illegal and pornographic content. Do you believe such a bill would be helpful?

Professor CANDEUB. Very much, Senator. As noted, OAMA doesn't really directly address the issue of de-platforming individuals. You could sort of read into it in one of the sections that it perhaps provides the protection, but it doesn't have direct language saying that the platform shall not engage in unreasonable discrimination.

Similarly, AICOA protects business users, but not user users. So I think that legislation that sets that forth would be a real step forward and would help Americans.

Senator LEE. Okay. Let's go back to AICOA for a minute. Professor Francis, AICOA's supporters have pointed out—they'll point to the requirement that, in many sections, conduct has to result in harm to competition. Does this alleviate any of your concerns?

Professor FRANCIS. It doesn't, Senator. And I think there's a real risk that a court looking at this bill will say, gosh, it's pretty clear that this was intended to signal a departure from the antitrust standard.

Number one, this conversation is being had right now as part of the legislative process. And so failing to answer that pretty strongly suggests that there isn't a clear answer that can be written into the bill. This is not itself going to be an antitrust statute. It doesn't use antitrust statutory language.

So, Section 7 of the Clayton Act, for example, talks about a merger being illegal if its effect may be substantially to lessen competition. That's not language that's followed here. And there's nothing in AICOA that says harm to competition shall be interpreted compatibly with antitrust.

So, this looks like a different kind of bill, doing different kind of work, that very intentionally is going a different way from traditional antitrust, including—because of political and other concerns about antitrust's consumer welfare standard itself. So I think failing to answer that question on the face of the bill is very dangerous.

Senator LEE. Okay. So, by leaving these important terms vague and undefined, are they giving the game away? Giving the game away in that this would end up being a bill about protecting competitors, not competition, or not consumers. Right?

Professor FRANCIS. I don't think there can be any room for doubt that if harm to competition in this statute is read to mean injury to rivals or injury to competitors, it would be terribly anticonsumer in its operation.

Senator LEE. And can that be remedied without an adequate narrowing of the term? Eliminating the vagueness in the terminology?

Professor FRANCIS. I can't think of an alternative, Senator, to saying—and it's a short and simple provision if this is really the purpose of the measure—to say that harm to competition means injury to consumer welfare, or not wedded to the terminology of something else, like overall harm to consumers and workers. But something that incorporates the concept, I think, is critical to ensure that it doesn't do a terrible amount of unintended harm.

Senator LEE. And yet this concept is not foreign to our competition policy. It's not foreign to antitrust law. This is pretty well-worn stuff. Right?

Professor FRANCIS. Exactly. As Professor Scott Morton says, that's what antitrust typically means when it says harm to competition. Now, it can be hard, in some cases, to figure out whether a harmful static effect, like a price increase, can really be outbalanced by a beneficial, dynamic benefit like greater innovation. So there can be difficulties in applying it. But everybody understands in antitrust that we're concerned with overall consumer welfare effects. And that's the question that's going to be asked of this statute.

Senator LEE. Thank you. I see my time has expired. Thank you.

Chair KLOBUCHAR. Thank you, very much, Senator Lee. Next up is Senator Durbin, our Chair. Thank you for being here.

Chair DURBIN. Thanks, Madam Chairwoman, Senator Klobuchar, I want to thank you, and Ranking Member Lee, for holding this hearing.

My observation, in general, is that the pace of change in the digital markets is lightning fast and evolving every day. My observation, based on many decades of working on Capitol Hill, is that the response of our Government is painfully slow, often understaffed and underinformed, and usually sailing against the wind of vested interest. It doesn't make a very easy situation for us to respond to in a thoughtful way.

I look back when I served in the House and we passed the Communications bill, about 30 years ago, and somehow left out the word internet. And I would think, as we reflect on the state of the digital market today and wonder how we're going to solve the problem, if smarter people or, at least, more people, are thinking about ways to avoid any kind of regulation or restraint, aren't going to get the best of us again. How can we avoid this? Open question.

Chair KLOBUCHAR. Does someone want to chime in? Mr. Lewis?

Mr. LEWIS. I'll take a stab at it, Senator. Senator, I think this is why—first of all, I agree with your assessment of the challenge for Congress to keep up with regulating a fast-moving sector.

And like the Communications Act, which you referenced, I think it's—a long-term solution is to look at empowering a regulator who has the expertise in the technology, like the FCC has in telecommunications, to be nimble, to be careful, to be analytical in the duties that Congress charges it with to protect consumers, to protect competition, and other harms, and with the proper oversight from Congress. So, we believe that's a critical part of protecting consumers online.

I know it's not the exact focus of this hearing, looking at specific competition bills, but I think added with the principles and ideas in these competition bills could be part of a real long-term solution.

And your point about not having the internet in the Telecommunications Act points to what I believe was the wisdom of Congress. The Telecommunications Act does give the FCC authority over communications over wire and radio. What else do we think the internet is? It's communications going over wire and radio. Sometimes it's a fiber optic wire. Sometimes it's radio signal to a mobile device. This is why we've advocated for authority over broadband at the FCC. But that's a different topic.

Chair DURBIN. But if we're dealing with digital markets so overwhelming in size—Amazon commanding 40 percent of the e-commerce market in the United States, 6 times its nearest competitor. Google controls 93 percent of online searches. Apple holds tight grip on 120,000,000 plus iPhone users. Do we really think the Federal Trade Commission is up to the challenge? Mr. Lewis, or whoever else——

Ms. LEWIS. I'm happy to——

Chair DURBIN [continuing]. Who wants to——

Ms. LEWIS [continuing]. Address that.

Chair DURBIN. Please, Ms. Lewis.

Ms. LEWIS. As somebody who's a former employee, enforcer at the FTC—and I know I'm not alone in that, as Professor Francis was also a former FTC enforcer—I absolutely think that the FTC and the DOJ are up to the task of applying the laws that we're discussing today, should they become law, AICOA and OAMA, to these markets.

More expertise is certainly better. Being more informed is better. But I believe strongly that the FTC and the DOJ, as they stand today, do have the tools and the ability to get the expertise that they need to address the problematic conduct in digital markets.

However, I'll say they have the ability, but they—I'll correct myself—they don't have the tools because—and that is wherein AICOA and OAMA come in. Current antitrust law is not well suited to address the problems that we're seeing—the abuse of these dominant platforms' market power. So these bills are really necessary.

But I'll also add that AICOA is a bill that, I think, did a lot of hard work—I think the Sponsors did a lot of hard work to futureproof the bill. So it is specific enough that it gives guidance to the agencies and the courts, but also leaves room for—to adapt to future conditions.

Chair DURBIN. Well, I just want to close by saying that no reflection at all on the Senator from Minnesota who has led this charge

and revitalized this issue of antitrust debate to a level that I've not seen in many, many years. And I think it's long overdue.

But I think the challenge for us is to make sure there is an agency with the authority, and the resources, and the political support, to get the job done. Thank you, Madam Chair.

Chair KLOBUCHAR. Well, very good. Thank you, Senator Durbin. I would note through the work that Senator Grassley and I did, and Senator Lee last year, the Merger Fee bill that passed with the 88 Senators, along with the Venue bill of Senator Lee's as an amendment, is going to amount to a billion dollars to these agencies.

As Professor Francis, he and I agree on this, on the resources, and what you're referring to, Ms. Lewis, that is a significant increase. While we'd like to see more, it's a significant increase, not on the backs of taxpayers, to help these agencies to do their work. Okay. Next up, Senator Grassley.

Senator GRASSLEY. Thank you, Madam Chairwoman. My first question is to Professor Morton, Mr. Lewis, and Ms. Lewis. In your testimony, you expressed support for the American Online Innovation Choice Act, how it deals with the digital market abuses.

You've just heard testimony by Professor Francis and Professor Candeub expressing a number of concerns with the bill. So I'd like to have the three of you briefly explain why you agree or disagree with Professors Candeub and Francis.

Professor SCOTT MORTON. Thank you, Senator. I think that the digital platforms we have today have quite a bit of entrenched market power. When Senator Durbin said technology moves fast, yes, it moves fast. But think of how many years we've been using Google Search, getting onto Facebook.com, having an Android operating system. These platforms have been around for some time now. And that's because we haven't been able to use current antitrust laws effectively to create competition in this space.

So, we need an additional tool. And if a few words describing what competition means is going to make this law pass for Professor Francis, then I think we're done. I mean, we've got problems, and we need solutions to those problems. A general-purpose antitrust statute would also be good. But because the problems in digital platforms are somewhat unique to them, and they're so entrenched, I think we need a particular tool. And this statute would be that.

Senator GRASSLEY. Mr. Lewis, if you've got something to add.

Mr. LEWIS. I agree. I think AICOA is very specific in the anticompetitive harms that it's trying to solve. Issues of self-preferencing, issues of tying, issues of control of data. And so I think the specificity that Mr. Francis is looking for is in the bill.

Regarding the concerns about free expression. Free expression is a core value for my organization. I believe that AICOA specifically targets anticompetitive harms, and I don't believe that content moderation on a platform—a single platform is necessarily an anticompetitive harm. Discrimination——

Professor SCOTT MORTON. You have other platforms to choose from.

Mr. LEWIS. Well, you do. And discrimination looks different on every platform. But the internet has infinite channels. And by pro-

moting competition, we're giving users a choice of platforms to go to.

And I know there's going to be another hearing on content moderation in the future. I think that's the proper place where folks who are concerned with too much or too little content moderation to address those concerns specifically.

But this bill dealing with anticompetitive harms has a secondary impact, that by promoting competitive choices, lets users vote with their feet and go elsewhere if they don't like the moderation choices that they're given on a specific platform. So, I don't think it's restrictive at all, and I don't find those choices to moderate content to be anticompetitive.

Senator GRASSLEY. Ms. Lewis.

Ms. LEWIS. Thank you. So, I do not agree with Professor Francis' analysis here. And I also, in terms of—there was a suggestion that adding consumer welfare—those words—into the statute of AICOA would be a good thing. I disagree with that. Consumer welfare is not a word that appears in any of our antitrust statutes, and can be interpreted to be extremely narrow and refer only to harms from price. Now, and certainly in digital markets, the harms go far beyond price to privacy and other non-price dimensions. So codifying that, I think, would be a mistake.

I also find it interesting that Professor Francis has said that the current antitrust laws is what we should work with and what we should invest in. Those laws, those statutes are extremely vague, very short.

And the language that was used in those antitrust statutes, well, that was new language, when those when those laws were passed.

Because it was using a new phrase, does that mean we shouldn't have passed those laws? So I think that what I see as a somewhat unfounded fear of courts interpreting harm to competition in a way that would prohibit procompetitive conduct. I don't think that that is a good reason to oppose this bill.

Chair KLOBUCHAR. Well, thank you. And thank you, Senator Grassley, for your work on the bill, the Merger Fees, but also for being the lead Sponsor on the bill that we're talking about today.

And I will note the hearing you referred to, Mr. Lewis, is actually going to be chaired by Senator Blumenthal. The Section 230 hearing with Senator Hawley—I believe, coming up tomorrow. So, we're on top of things. Okay. Next up is Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman Klobuchar.

And let me start with a particular welcome to Ms. Lewis. As a friend, colleague, and admirer of David Cicilline's, I'm very glad that you are here, and thank you for his work supporting the efforts of the House Judiciary Committee.

I have two questions, and given the short period of time, I would invite specifically Ms. Scott Morton, Mr. Lewis, and Ms. Lewis, to answer as questions for the record. But given that, we'll have a little bit of time, I invite you to jump in.

The two questions are, first, we have the EU's Digital Markets Act coming on, and I'm interested in what effect you see that having in this marketplace, and what lessons we should take from the effect of that law in this marketplace. Presumably, the minimum conclusion one could draw is that you can legislate in this space

and not break everything. But I'd be interested in your views about that.

And the second, to the point suggested just now by Chairman Klobuchar, is how do you see Section 230? As problematic or helpful in this space? And I'll flag my bias. I think it's problematic. I think a lot of these problems would have sorted themselves out a lot earlier if these industries weren't protected from several centuries of legal tradition that govern human behavior, so——

Professor SCOTT MORTON. I'll just jump in on the DMA quickly——

Senator WHITEHOUSE. Please.

Professor SCOTT MORTON [continuing]. And say that it's going to be very interesting for the United States to see how platforms respond to the DMA. Because there will be some instances, I imagine, where it's easier, more cost effective to have one business model and run it globally. In which case, the changes made to comply with the DMA will be taken advantage of by American consumers——

Senator WHITEHOUSE. Yes.

Professor SCOTT MORTON [continuing]. And businesses. I can also——

Senator WHITEHOUSE. We see that in automobiles when California——

Professor SCOTT MORTON. Correct.

Senator WHITEHOUSE [continuing]. Puts its standards out.

Professor SCOTT MORTON. Exactly.

Senator WHITEHOUSE. Nobody makes two cars.

Professor SCOTT MORTON. Exactly. But there will be other cases where, look, if the platform can run an exploitative model in the United States and a competitive one in Europe, and they make more money doing that, then they'll choose to do that. And so we're going to see those kinds of choices as well as then be able to learn from the smoothness, or lack thereof, in new products, or lack thereof, as to what are the most effective rules.

Senator WHITEHOUSE. And who do you expect most effectively to look at that behavior and draw lessons from it in the U.S. Government?

Professor SCOTT MORTON. In the U.S. Government?

Senator WHITEHOUSE. Mm-hmm.

Professor SCOTT MORTON. I don't know. I mean, the European Commission is going to get reports from platforms and confidential information on what's changed and what they're doing. I don't know that we have any way to study it in the U.S. Government——

Senator WHITEHOUSE. Do you think——

Professor SCOTT MORTON [continuing]. That I'm aware of.

Senator WHITEHOUSE [continuing]. The FCC would be up to the task of looking at that.

Professor SCOTT MORTON. Would who?

Senator WHITEHOUSE. The FCC.

Professor SCOTT MORTON. That would be a great idea. Ask them to write a report. Yes.

Senator WHITEHOUSE. Okay. Mr. Lewis.

Mr. LEWIS. Senator, you asked about Section 230.

Senator WHITEHOUSE. Yes.

Mr. LEWIS. While we're very supportive of these efforts to promote competition, I think Section 230, and the issues around it, are a different issue. Section 230 was crafted to support the creation of third-party content online—both the choice to moderate it and the choice not to moderate it.

And I think it's an essential protection that, combined with smart competition policy, actually gives folks choices to express themselves freely on whatever platform they choose to, based on the moderation practices that that platform uses.

I think transparency of those moderation practices is important. I think due process is important. But it's——

Senator WHITEHOUSE. I guess you and I are going to disagree on that.

Mr. LEWIS. We might disagree. Yes.

Senator WHITEHOUSE. Ms. Lewis.

Ms. LEWIS. Thank you. So you asked what lesson could be learned from the enactment of the DMA. I think one important lesson is what you referenced is, we see that you can pass legislation here to rein in the dominant digital platforms and stop the abuse of their market power over businesses and consumers.

And you can do that without breaking these products and services that consumers love. These two things are in no way mutually exclusive. And so we are already seeing, or at least it was reported, for example, that Apple—who said if we pass OAMA, we're going to break the iPhone and the App Store system, and create problems for users, in terms of safety and security.

Well, it turns out or, at least, it's reported that in Europe, in order to comply with the DMA, that they are preparing to allow for alternative app stores. So, how is it that—you know, it's interesting that they say here last Congress, to U.S. Members, oh, you cannot pass this law. It will break the product. It will break the phone. And then there are reports that they're voluntarily agreeing to make these changes. I will say not purely voluntarily because it's in response to the law.

And if we want to see similar benefits for U.S. consumers and businesses, then I think we similarly need to pass legislation.

Chair KLOBUCHAR. Thank you, very much. And thank you for that excellent point, Ms. Lewis, because I just don't think we're just going to wait and let Europe have the benefits for 10, 15 years.

They're not going to do it unless we start moving, and then maybe they'll negotiate with us. Okay. Next up, Senator Blumenthal, who knows a little bit about this topic. Thank you.

Senator BLUMENTHAL. Thanks, Madam Chair. And thank you for your profoundly persistent and courageous work in this area. Thanks to our Ranking Member, as well. I'm very proud to be working with you on a number of these bills, including your American Innovation and Choice Online Act, which does far more than just stop self-preferencing. It is very, very potentially significant.

And my Open App Markets Act, the reference was made earlier to Section 230. Yes, we are having a hearing tomorrow—Judiciary Committee hearing, the Tech and Privacy Subcommittee. Senator Hawley and I are going to be exploring potential reforms to Section 230.

But let me just begin with the comment that Senator Klobuchar just made. If we wait for Big Tech to reform itself, we're going to be old men and women. We may not be around to see anything happen. And to the point about content moderation, let's be very clear. Big Tech has an abysmal record on civil rights and safety. It helped foster and fuel racial discrimination, threats, and privacy violations that have a material and costly impact on people's real lives.

These behemoth corporations are not protectors of vulnerable communities nor of free expression. So if we wait for them to do that as well, we just are not going to see it. There is an elephant in the room, which is Big Tech's response to this legislation. And I'm not speaking for Senator Klobuchar, just for myself. I would say it's an unprecedented smear campaign, a disinformation strategy. One of the elements of that disinformation campaign is to say, it's a dire threat to cybersecurity and privacy.

As anybody who's read both of our measures knows, we take specific steps. We insert very explicit provisions, which Big Tech says need to be much broader, trying to create loopholes and exceptions that swallow the rule.

I wonder, Professor Scott Morton, whether you would describe—you allude to some of them in your testimony. And I know you're not a lawyer. I always think of you as a lawyer because you know so much more law than most of us on the Judiciary Committee—speaking, again, just for myself—but you're also a very astute and learned economist. I wonder if you could talk about how those exceptions provide for privacy and security?

Professor SCOTT MORTON. Thank you, Senator. I always get a warm welcome from the Senator from Connecticut, which I appreciate. The important safeguards in these bills, I think, are doing exactly what you say. It would be counterintuitive to have a bill that's going to promote consumers' welfare and have there be dangerous products.

And therefore we want to give the platforms the ability to control that. And there are many ways to do that. And it is in the platform's interest to do that because if you want to attract users to your platform, you want it to be safe and a good experience.

So, I just see no reason why with all the technological capability these platforms have, they can't design the product to be safe. And given that both bills allow them to do that, I'm really thinking that American ingenuity is going to make this work out just fine.

Senator BLUMENTHAL. Thank you. Ms. Lewis, you made the comment just now that Apple may be developing a system to enable apps access to their phones in Europe, but I'm not sure we can count on those products being available here. Shouldn't Americans have as much access to competition, fair play, innovation, as European consumers?

Ms. LEWIS. Senator Blumenthal, I agree with you 100 percent. And the—it is just critical that American businesses and consumers can benefit from the increased choice in terms of alternative app distribution. And this would also likely result in not only cost savings for consumers, but also spur innovation and growth among U.S. companies. And so it is U.S. consumers, and it is also U.S. businesses.

The U.S. economy does not just consist of these four dominant platforms. And so if we want to see the economy thrive and our consumers benefit from competition, then legislation must be passed in the United States to do that.

Senator BLUMENTHAL. I'm at the end of my time. I have a bunch of other questions, but I just want to thank all the members of the panel for being here today and your last comment. These measures are really pro-business. Maybe they're not pro-monopolist or pro-predatory conduct, but they are pro-business. And as complicated as it seems, the internet befuddles a lot of people.

Think of it in terms of the old days of the railroads. If the railroads had said you can only run our boxcars with only our manufactured goods because we control the rails, you didn't need any smoke-filled rooms to know that was going to be anticonsumer and anti-business. Thank you, Madam Chair.

Chair KLOBUCHAR. Thank you very much, Senator Blumenthal. Someone else who knows a lot about this, has been a leader in this area, Senator Hirono is with us. Thank you.

Senator HIRONO. Thank you, Madam Chair. It's so good to be on the Subcommittee, and I thank the Ranking Member also. It's been really challenging to do anything to regulate these very powerful digital platforms. So, the AICOA bill, when we start talking about making changes to Section 230, it's just been almost hellacious, I'd say.

So, I think Professor Scott Morton, you said something along the lines of the current antitrust law have not been particularly effective in regulating digital platforms. Did I hear you correctly that you said something along those lines?

Professor SCOTT MORTON. Yes, I did.

Senator HIRONO. Mr. Lewis, do you agree with that kind of characterization of the current antitrust laws?

Mr. LEWIS. Yes.

Senator HIRONO. So, what if AICOA, which is, I think, pretty specific in what it wants to do, would it help to have a law like that, which is much more specific than the current antitrust laws?

Professor SCOTT MORTON. In my opinion, it would. And that's because the current antitrust laws have requirements such as defining relevant markets and predicting but for outcomes that turn out to be quite challenging in fast-moving digital markets. And if Congress wants better enforcement here, I think it's very helpful to give more explicit instructions to courts on how to get there.

Senator HIRONO. Mr. Lewis, did you want to add something?

Mr. LEWIS. Just the thought that, you know, these are often referred to as antitrust bills, but they're very specific in the prohibited conduct. And that, part of what we've seen in the weakness of the current antitrust laws, is just how they've been interpreted.

And so I think there are ways in which, with cases brought that challenge monopoly under the current antitrust laws, to look at different ways to think about the power of monopoly. But this specific bill, AICOA, I think, adds just more tools to the toolbox for those antitrust enforcers.

Senator HIRONO. Oh, back in the day when the Sherman Act and Clayton Acts were passed—and, yes, we have decades of interpretation of both of these laws—but nobody predicted that we would

have these kinds of hugely powerful digital platforms that—that millions of people use. And basically, there's very little, apparently, that we can do to make sure that consumers are protected.

And so, Mr. Lewis, you mentioned that Public Knowledge has called repeatedly for a new competition promoting expert regulator for digital platforms. And I think that is acknowledging that maybe we need a whole new kind of legal framework for regulating digital platforms. So, can you just explain a little bit more about what you had in mind with that proposal?

Mr. LEWIS. Sure. The idea of an expert digital regulator is to complement antitrust enforcement, not to replace it. And a regulator, we think, would have authority over consumer protection, authority over, or involvement with, competition harms and concerns.

You know, my background is in telecommunications. We're impressed with the relationship between the FCC and the antitrust enforcers——

Senator HIRONO. Mm-hmm.

Mr. LEWIS [continuing]. Where they work together when looking at mergers, when looking at—you know, with a different standard at the public interest harms. And so an expert digital regulator would be able to do that to address things that can't be dealt with through competition policy.

So, you know, I think it could be structured in a number of different ways. It could be an existing agency. It could be a new agency. There's interesting proposals out there from Senator Bennet and Senator Welch that we're interested in and supportive of. It's a challenge to set up. But I think taking the time to look through the harms that you want an agency to address, and giving them the proper authority to do so, and the resources to do so, I think——

Senator HIRONO. My time——

Mr. LEWIS [continuing]. Would help Congress. Yes.

Senator HIRONO [continuing]. Is running out. Thank you.

Ms. Scott Morton, would you agree that perhaps a new kind of agency, or a person or two, to be focused on consumer harms and the public interest——

Professor SCOTT MORTON. Yes, I do.

Senator HIRONO [continuing]. Would rein in digital platforms?

Professor SCOTT MORTON. It's what we normally do in the United States. We invent airplanes, we have an airplane regulator. We invent trains, we have a train regulator. We invent drugs, we have a drug regulator. There's no regulator for digital, and there's a lot of problems as a result. So, I agree.

Senator HIRONO. I agree with you. Thank you for talking about that.

And Ms. Lewis, you noted that the DMA that Europe has passed, the companies are able to make the appropriate adjustments.

So, there's nothing to say that we can't pass something that is—the AICOA is narrower than the DMA, isn't it, in its focus?

Ms. LEWIS. To give you a more complete answer, I would want to get back to you in writing. But, I think—I think it is, the AICOA is narrower, and I have done a comparison of that.

Senator HIRONO. Oh, thank you. We would appreciate having that. But the world is not going to come to an end because Europe passed the DMA. Thank you, Madam Chair.

Chair KLOBUCHAR. Okay. Very good. Thank you. Next up, Senator Padilla.

Senator PADILLA. Thank you, Madam Chair. And particularly, I want to thank you for your leadership on these issues.

I think it's vitally important, not just for the innovators, and investors, and entrepreneurs, but for consumers, and workers, and the overall health of our economy, that we have an open, and innovative, and competitive technology sector.

So, I hope we can continue to work closely together, this Congress, to build upon the great work that has already been done to better identify market failures, and areas of underenforcement, and to develop more precise legislative remedies to specifically address the issues that we're facing.

Now, during the Committee's consideration last year of the American Innovation and Choice Online Act, I expressed concerns that provisions of the bill may open the covered platforms to either lawsuits, or even threats of lawsuits, for decisions they made to enforce their content moderation policies against hate speech, misinformation, and other content that they may want to not host.

And several academics, nonprofit groups, and other Senators, actually voiced similar concerns. And even supporters of the bill approached my office with differing opinions. I was told by some supporters that no such problems existed, while other supporters told me that, yes, the concerns raised were indeed valid.

Question for Professor Francis. Should we be concerned about the bill's unintended impacts on platform content moderation, and is this an area where the bill can be improved through additional clarity?

Professor FRANCIS. I think so, Senator. I'm certainly not an expert on either the practices or the law of content moderation. But as I read this bill from the perspective of an antitrust person thinking about what compliance would look like, I look at two things, and they both give me the concern you've just articulated.

So, one is Section 3(a)(3) of the bill, which prohibits discrimination with respect to the application or enforcement of terms of service in favor of business users against similarly situated business users.

Now, as I read it, that would include content moderation of various kinds that a court ultimately concluded, or even a State attorney general alleged, was discriminatory.

And then we look at our affirmative defenses. AICOA provides no defense on the ground that what was restricted was spam, was supplying false, or objectionable content. Nothing in there that one might plausibly identify with content moderation. So, regardless of how one feels about the optimal content moderation law, this very sharply raises the question, but doesn't answer it.

And to my mind, what that means is litigation, threats of litigation, a lot of uncertainty, and a lot of deterrent effect running in ways we almost certainly don't want.

Senator PADILLA. Well, the American Innovation and Choice Online Act, as we discussed and debated in the Committee last year, attempts to address several market problems at once.

However, I worry that in doing so, it may inadvertently do harm to products and services that consumers actually enjoy. For example, in broadly and presumptively making unlawful the preferencing of a platform's own product, services, or lines of business, is it possible that basic and convenient features of integrated products and services that consumers enjoy, and benefit from, would be prohibited, and subject to unnecessary and, perhaps, chilling scrutiny? Professor Francis, I'll let you go first here.

Professor FRANCIS. I completely share that concern. So things that would constitute self-preferencing cover an array of things that are clearly great for consumers. Integrating functions like map results in search. Or better integrating your own voice assistant because you found a way to do that.

Pre-installing apps or features on a device without doing that for the whole world. Bundling services together, or even, in order to create a more secure and seamless experience, just say, hey, we're going to have a closed system on this part of our platform where we're not going to have third-party participation.

All of that stuff is self-preferencing, and then the whole game is whether or not there's harm to competition. Number one, that term is central and undefined. If nothing else, that is a ton of uncertainty, and the prospect of being dragged through investigations, litigations, injunctions, huge penalties, and even having executive personal compensation taken away, that's going to deter a lot of behavior that we would want to see from platforms that they'd otherwise do.

Senator PADILLA. Well, I'll just conclude with this, Madam Chair, because I still agree with the stated objective here of our legislative efforts. But I want to continue to work with you, and the experts here, to make sure that we're getting it right. Thank you, Madam Chair.

Chair KLOBUCHAR. Thank you, very much.

So, Professor Francis, you said you were not an expert on the content moderation. So I'm going to turn to some people that I think could shed some light on it, but I appreciated your answers.

Ms. Lewis and Mr. Lewis, we'll turn to the two Lewises here, could you talk about what this bill is about, the American Innovation and Choice Online Act?

And I'll start with you, Ms. Lewis, whether or not the bill would have impact on the speech rights of anyone on a covered platform. I point out that Senator Grassley and I worked to ensure that the bill is focused solely on addressing digital platform competition issues. But that, of course, hasn't stopped the bill's opponents from raising dubious arguments related to free speech. And so I thought you, Ms. Lewis, might want to address that. So, please, go ahead.

Ms. LEWIS. Yes, thank you, Senator Klobuchar. Unfortunately, I think that this debate over content moderation or, sort of, the critiques that are aimed at AICOA, are a divisive distraction. In my view, AICOA does not impact content moderation. It does not make it harder for a gatekeeper platform to engage in content moderation, and it does not make it easier for the digital gatekeeper to en-

gage in content moderation. The bill simply has nothing to do with it.

And in terms of the idea that certain things may be—you mentioned the word, "dubious," and the idea that certain things may be possible, I would not even concede that it is possible. But let's say it is possible that a State AG, or I, could interpret the bill in that way. I don't think it's plausible. And I don't think—when we think about very unlikely things that could occur and possible farfetched outcomes, I think we should be thinking about what is plausible rather than what is improbable and unlikely. Again, in summary, AICOA does not affect content moderation.

Chair KLOBUCHAR. Thank you. Senator Padilla had to leave, but we will convey your testimony to him. Mr. Lewis, do you want to answer that as well?

Mr. LEWIS. I guess what I would add, because I agree with Ms. Lewis, what I would add is just that the language in the bill is so specific. Mr. Francis keeps pointing to the competition harm phrase. But I think it's very important that the Attorney General, the Federal antitrust official, would have to go to court and make a case for what is materially harming competition in the practice of the platform. And so I don't read that phrase as referring to content moderation. But if someone wants to bring that case, they would have to point to what that practice is.

Simply limiting someone's content that they posted online, I don't see how that hurts competition when there's so many places where you can post online, and folks can create their own websites. So there's a great opportunity to speak. So, proving that case just seems very hard. I think that's what Ms. Lewis——

Chair KLOBUCHAR. Right. Yes.

Mr. LEWIS [continuing]. Means by impractical.

Chair KLOBUCHAR. We also note that the Attorney General, the Justice Department, supports this bill as well, so.

Mr. Lewis, again, kind of changing topics here. Numerous reports have suggested that Amazon creates knockoffs—these are, you know, Wall Street Journal stories and the like—of third-party sellers' products and uses its algorithm to give its own brands an advantage.

A recent study by economists at the National Bureau of Economic Research found that Amazon-branded products are ranked higher than observably similar products in consumer search results on Amazon's platform.

How do these practices affect competition and the incentives of small businesses to create new innovative products, and how can some common-sense rules of the road—maybe you want to start with this—help protect small businesses to compete against these mammoth companies?

Mr. LEWIS. Right. I think the rules in AICOA go a long way to protect those practices. The difference between an online marketplace, like Amazon, and a brick-and-mortar marketplace are very different. The ability to control data, to see all the data that's coming in about sales, about the products, the limited space, and the control of that space where products are seen, is just very different.

The scope and scale of an online marketplace is just wholly different from what we see in brick and mortar. And so having these

sort of specific rules protecting the small businesses and the products that they want to bring to that market since it's one of their few choices that they have to reach consumers is critically important.

Chair KLOBUCHAR. Mm-hmm.

Maybe I'll ask you this—it looks like, Ms. Lewis you want to say something, but I want to—just very quickly.

Ms. LEWIS. Yes. So, I think the self-preferencing that you just mentioned is a perfect example of what can be anticompetitive self-preferencing. And so you have the situation where Amazon is putting its thumb on the scale to distort competition. And that's the situation where third-party sellers, who maybe come up with new ideas, or have high quality, maybe better-quality products, are not being able to compete on the merits of their goods and services——

Chair KLOBUCHAR. Okay.

Ms. LEWIS [continuing]. Their goods, in this case.

Chair KLOBUCHAR. All right. And then I just want to make—you mentioned these conflicting statements. And if you could just quickly mention this. I think this is so important. We made it clear in the bill that it would not impact subscription-based services like Amazon Prime, despite Amazon's claims. And I noticed these lying pop-up ads that I've shown to my colleagues because that's what they're done—they're done to scare other people if they support the bill.

And so now, Amazon in Europe has pledged to allow sellers to use other shipping and logistics services and still be part of Amazon Prime. And they are doing this to settle an investigation by the European Commission.

The exact thing that they said would break Prime in the U.S. That's what their claims are. How do we square the story Amazon is telling us here in the Senate, and what they are actually doing in Europe, and what they're doing to our consumers versus what's happening in Europe?

Ms. LEWIS. Unfortunately, I think it's an example of doublespeak. I understand that Amazon has incentives to want to hold on to the profits that they may—and the revenues that they may get from self-preferencing. And in doing so, perhaps they overreached in their arguments to regulators and legislators here.

But the proof is in the pudding. If they are offering this up, they offered this up as a voluntary commitment that, in fact, they can do this and still continue to offer Amazon Prime, there is your answer. I'm not sure how to square it other than that the original argument was disingenuous.

Chair KLOBUCHAR. Okay. I have another question about another hypocrisy, but I'll go in, to let Senator Lee go.

Senator LEE. Thanks. Professor Candeub, did you want to respond to that last point we were talking about? I think there was a hanging chad there somewhere.

[Laughter.]

Professor CANDEUB. The content moderation issue?

Senator LEE. Yes.

Professor CANDEUB. Yes. I think it's an interesting question, and it does go, as correctly pointed out, to the Section, I guess it's 3(3), that prohibits a platform from discriminating in the application

and enforcement of the terms of service of the covered platforms amongst similarly situated business users——

Senator LEE. I'm having a hard time hearing you, again.

Professor CANDEUB. Oh.

Senator LEE. Can you move your microphone?

Chair KLOBUCHAR. Could you move your microphone?

Professor CANDEUB. Yes.

Senator LEE. Yes, thanks.

Professor CANDEUB. Is that better?

Senator LEE. Yes, that's better.

Professor CANDEUB. Okay.

Senator LEE. Thanks.

Professor CANDEUB. So it goes back to the Section 3 that prohibits discrimination among similarly situated business users. And so what does that actually mean in life? Well, you could imagine, you know, a dating app that only is for, you know, Nazis, or, you know, Communists, or something like that, and a platform didn't want to have it. And the question is, what would be the remedy? I think it was pointed out they would not have a private right of action. I mean, you'd have to find some attorney general or the Department of Justice to take up their cause, which I would find extremely unlikely. So, you know, I do that in the abstract. It does present this problem. But I think, in reality, it's not something that is likely to occur.

Senator LEE. Right, right. And if it were to occur, we're talking about a very weird niche market. I mean it——

Professor CANDEUB. Yes.

Senator LEE [continuing]. One that, that would not likely amount to a significant percentage of the population, everyone would hope. And so if you ended up in that circumstance, you'd be dealing with something different than where you have politically motivated content moderation decisions that may cut against where roughly half of Americans are excluded from it. Is that part of your point?

Professor CANDEUB. Yes, precisely, because there is no private right of action. I mean, you'd have to have the judgment and common sense of elected officials, and I would be very surprised that they would take up that cause.

Senator LEE. Right. All right, back in 2021, Apple, Google, and Amazon, as you mentioned a little while ago, de-platformed Parler. This, of course, was a popular and quickly growing competitor to Twitter that was favored by many in the sort of libertarian-to-conservative community.

Conservatives have, of course, been lectured for years that if conservatives don't like how a tech platform moderates content, then they should just go build your own, as many of us were told.

So the Parler example, I think, illustrated how shallow and how empty that response would be. Do you agree that Google and Apple ought to be barred from preventing users from installing apps of their choice on their devices?

Professor CANDEUB. I think that's a reasonable, targeted remedy. As I pointed out, Google and Apple are only able to skew public discourse because of the market power they enjoy. I think a targeted solution that says, you know, look, you are—you're unusual. You're sui generis. You're the big guys. We all depend upon you. You have

general obligations to the institutional values of the United States. And I think that would be a targeted and limited approach that would be effective.

Senator LEE. Part of what has left so many of us cynical about what happened with Parler is the fact that Parler was—it had hit its sweet spot. It had hit its stride. It was doubling. I don't remember what the stats were, but it was doubling its user base every 6 weeks, or something like that. It was growing by leaps and bounds. And all of a sudden in early 2021, out of the clear blue, some tech giants combine together and all decide, as if miraculously, that they're going to shut them down. And they do shut them down.

Now, they make decisions eventually that allows Parler to come back, but by then, the party is over. By then, it had lost the vibe. And, you know, these things are such that if you cut that off at the wrong time, and you take them essentially offline for a couple of months, it's a death knell. And they've never recovered as a result.

Professor Scott Morton, could we have avoided the situation that we're in today if we had just had better enforcement of our antitrust laws over the last 10 or 15 years or so?

Professor SCOTT MORTON. Thank you, Senator. I think the answer is not so much enforcement, but the jurisprudence in the courts. When you have rules like *Brooke Group*, and jurisprudence like *Amex* and *Trinko*, it really sets such a high bar for the plaintiffs that you can have very good enforcers, but they just aren't going to win in the places where the consumer needs them to win.

Senator LEE. Do you think that the antitrust law has been weakened by lax enforcement? Is that part of your point?

Professor SCOTT MORTON. No. I think it's been weakened by a tradition that's very old now, from the *Chicago School* in the 1970s that made a lot of assumptions for courts. Like, markets will self-correct on their own. You should be really afraid to enforce that—that predatory pricing doesn't exist. Oligopolists can't collude—things that we know to be actually not part of the economic learning that we have and not part of how markets work.

But if you make those assumptions, you don't need antitrust enforcement. And courts have been therefore dialing it back really quite steadily over the last 40 years.

Senator LEE. Professor Francis, how do you respond to the same question?

Professor FRANCIS. I agree with, I think, almost everything Professor Scott Morton said. I think, you know, a lot of the criticism that has been leveled at enforcement agencies would better have been leveled at the decisions of the Federal courts on some important margins in the last couple of decades.

But I'll add that I also think part of the problem is that our statutory standards, even though we've been working on them for 130-odd years, in the case of the Sherman Act, could really use some clarification. Right.

So 1890, the Sherman Act gives us restraint of trade and monopolies. Those are still battlegrounds in litigation today. 1914, the Clayton Act substantially lessened competition. The courts, for sure, have been taking—you know, antitrust cases should be hard to win, but they shouldn't be impossible to win. So courts have

been unduly, sort of, receptive to defendant arguments for several decades.

But it's not just the courts. It's also the fact that they're looking at statutes that really could be clarified by Congress in some pretty common-sense ways that I think would really sharpen antitrust on some very important margins: monopolization law, merger law, in particular.

Senator LEE. And doesn't that suggest that a lot of these problems could, and should, be dealt with most appropriately through reforms to the way we enforce them? Reforms like those suggested in the TEAM Act rather than implementing expansive, untested new regulatory regimes?

Professor FRANCIS. I think that antitrust enforcement, not just for a small number of tech companies, but across the economy, is the most important competition policy problem we face right now and an urgent need. And I want to just respond to the idea that AICOA is a kind of fast-track antitrust, it really is not. Antitrust enforcement focuses on the use of market power in ways that harm consumers. When you consider all procompetitive justifications for a practice, it would be protecting interplatform competition here, making sure that we weren't suppressing or deterring the emergence of competitors of Google, and Facebook, and Apple, and others. And it rejects the kind of blanket duty to deal that AICOA imposes. So it's not——

Senator LEE. So it's almost anti-antitrust.

Professor FRANCIS. That is——

Senator LEE. Double——

Professor FRANCIS [continuing]. Exactly——

Senator LEE [continuing]. Negative. It's just a trust at that point.

Professor FRANCIS. It turns the trading partners of these platforms, who would be the very businesses best placed to become or to sponsor competitors, into stakeholders in the status quo. And not only is this not antitrust, it's not even accelerated antitrust.

If Congress passes this bill, we're going to see a generational landslide of litigation over concepts like critical trading partner, fair and neutral search rankings, preference—part of, or intrinsic to, a digital project. The mechanism of enforcement is the same as antitrust. We're going to see enforcement actions brought by agencies moving through the Federal court at the same pace as antitrust but doing less good.

Senator LEE. So 133 years later, we're still arguing over meaning of things enacted in 1890. If we enact other language, you know, sure, we're still haggling over it, but we have developed, over time, a pretty sound understanding of what they mean. If we develop this, this could be another 130 years of exploratory litigation. It would be really good to fund the private college educations of the children of lawyers everywhere but could create chaos.

Professor FRANCIS. This is going to cost the economy a fortune in compliance costs and attorney fees, even before we get to foregone innovations or failure to protect consumers. I would love to see us take a fraction of that money and use it to support antitrust enforcement.

Senator LEE. All right. Let's talk about the Open App Markets Act for a minute. It, of course, banned dominant app stores from using MFNs. Would this help bring more competition to that space?

Professor FRANCIS. I think it could, Senator. And one of the things that I like about it is that this promotes interplatform competition. So the idea is that if you take away the power of an app store with market or monopoly power to say to app developers, hey, don't offer a better price elsewhere—if you take away their ability to do that, then suddenly big app developers can sponsor competition against the app store itself by offering discounts or other preferred terms. So I would support an MFN ban here, as in other markets with market or monopoly power.

Senator LEE. Professor Lewis, would AICOA prevent a company like Amazon from charging different prices to business users on its platform based on a user's size?

Ms. LEWIS. Oh, I'm sorry. Ms. Lewis. I'm not a professor, but——

Senator LEE. I'm sorry.

Ms. LEWIS. That's okay.

Senator LEE. Today you are.

[Laughter.]

Ms. LEWIS. I'm sorry. Could you repeat the question?

Senator LEE. Yes. Would AICOA, as you read it, would it prevent a company like Amazon from charging different prices to different business users on its platform based on their size or the volume in which they deal?

Ms. LEWIS. So, on it, my—my reading of it is that it would not, but I would want to go back and really do an analysis to look at the statute and confirm that that's accurate.

Senator LEE. Do you think it's unfair to charge different businesses different prices based on their size?

Ms. LEWIS. So, again, I think I would have to give that some more thought because there's really—there's no context there. So I would really want to look at the individual facts of the situation before I would make a blanket statement.

Senator LEE. Okay. Professor Scott Morton, let's go back to you for a minute. AICOA would require enforcement actions to be brought in Federal court. While I've got concerns with the breadth of the bill, I view this element as absolutely essential to protecting due process. Would you agree with that?

Professor SCOTT MORTON. Yes, that's right.

Senator LEE. What in your view—are there things that would be better than this, or is this the right thing to do it?

Professor SCOTT MORTON. Well, I think as I said in my statement, in some ideal future world, we have a regulator who is expert, and can use the public interest standard, not just competition, but privacy, security, all these other issues you've been raising.

In the absence of that regulator, I'm against the status quo. I think we should try to move forward with a bill like this. I think the possibility of public enforcement, rather than private enforcement, limits the kinds of cases that are being brought to ones that are meritorious and necessary.

And so with luck, you wouldn't get platforms engaging in litigation where it's pretty clear that the instructions in the statute require them to do something.

Senator LEE. But do you think it would be preferable to have them handled by experts in an enforcement agency, sort of, a beefed-up panel of uber-experts?

Professor SCOTT MORTON. Well, as I said, when we invent technologies, typically, in the United States, we also bring a regulator along with them—whether that's trains, or pharmaceuticals, or airplanes, or whatever. And I don't think this technology is any different in that regard.

But it usually takes Congress a really long time to regulate dangerous things. I don't know why that is. You probably do. And so in the meanwhile, I think something like this, where we're working through the courts and building off of what we know from the antitrust context, is an excellent first step.

Senator LEE. Okay. Thank you.

Chair KLOBUCHAR. Very good. Senator Blumenthal.

Senator BLUMENTHAL. Yes. Just a couple of quick questions. First, let me just say on the issue of enforcement, you know, I spent most of my career in enforcement. Some of it, in fact, in antitrust enforcement as State attorney general. So I'm all in on enforcement.

And I'm also—frankly, I've been critical of Federal antitrust enforcement.

Often the States were ahead of the Federal Government in some cases on antitrust enforcement, which I say with some pride as a former State attorney general. But enforcement can't invent laws. You know, people used to say to me, "Oh, you're too aggressive," even when we won cases. And I used to say, "Well, it's not me that gives us the power, it's the law. I can't do anything without the law on my side."

So when we talk about clarifying or improving, we're just giving enforcers the tools that they need. And some of it is to avoid those loopholes, and exemptions, and exceptions that can swallow the rules.

Let me ask you Professor Scott Morton, and others can answer too. I understand that there have been media reports indicating that the Department of Justice is investigating Apple for some of the same exclusionary and tying practices that the Open App Markets Act and the American Innovation and Choice Online Act would help to prevent.

Why should we not just rely on the Department of Justice to try to enforce existing law at some point, I don't know, a year, 2 years, 5 years, a decade from now?

Professor SCOTT MORTON. Well, I think you've answered your own question. The *Google* search case, that was filed in 2020, hasn't come to trial yet. Typically, a case takes some years of investigation before it's brought. Then the court needs to write an opinion. Then there's an appeal, and it goes from there. And at the end of that process, it's not clear what the remedy is, because the platform has become so entrenched, over so long, that it's really hard to do anything to restore the lost competition.

So that's why I think this bill is really useful, because it holds out the prospect of much more immediate relief for consumers. We would have competition on the platform, in short order. And I think that's both safer and quicker for consumers.

Senator BLUMENTHAL. Well——

Professor FRANCIS. Senator, do you mind if I accept your invitation——

Senator BLUMENTHAL. Yes, please do.

Professor FRANCIS [continuing]. To add something? I can't understand why anyone thinks AICOA enforcement will be any faster than antitrust enforcement. It's going to be complaints filed in the same Federal courts, proceeding under the same discovery rules, on the same slow timetables. Except, all the terms are new, and don't have the benefit of 130 years of precedent and doctrine to guide them.

This is not like the DMA. To make the DMA work, the institutional structure of the European Union is critical. The European Commission proposed it. They issue implementing Acts to tell specific companies how to comply. They conduct compliance audits. They take enforcement actions, and then they issue decisions on them.

So, there's only one actor that has a bureaucratic monopoly on the process. And whether or not one likes that system, that is not our order.

Ms. LEWIS. I——

Professor FRANCIS. So, I don't think this would be faster at all.

Ms. LEWIS. I disagree——

Senator BLUMENTHAL. Ms. Lewis.

Ms. LEWIS. I'm sorry. I disagree with that characterization. I mean, one important thing that AICOA and OAMA both do is to absolutely streamline one concept that is extremely time consuming, and expert intensive in antitrust law, and that is market power.

And so AICOA has a definition of critical trading partner. And yes, it may be litigated, the scope of what that means, but Congress is telling the agencies and the courts what it means. There is a description and explanation of that.

When it comes to OAMA, the word "competition" is not there. There are much fewer terms to interpret. It is a bit more straightforward because it is much narrower. And for OAMA, there is no need to prove a relevant market definition, to assign market shares, and so both bills, I believe, would streamline the process. I'd also add that the DMA, once it was passed, it already—the idea is to avoid litigation here by making clear what conduct is prohibited.

And so I think you would expect to see changes. Companies will respond differently. But some of these digital platforms, I believe, will, if these laws are passed, make changes that will benefit consumers and businesses in response to that.

Senator BLUMENTHAL. Yes. I think, Professor Francis, your comment is correct. The rules of discovery are the same. The rules of evidence are the same. The Federal procedure is the same, but the cause of action is different. The cause of action is targeted and streamlined.

So, you may have discovery, but it's not going to be on a kitchen sink. It can be on literally one topic, and it can be streamlined. The whole process can be streamlined.

And equally important, the remedy is clearer. A lot of the litigation—you take the *Microsoft* case, which I was involved in, half the litigation was about the remedy. The judge ordered the company broken up. He found liability. The court of appeals reversed. And frankly, we didn't ask for the company to be broken up.

So, you know, it's—I think it comes down to the cause of action, defining what the wrong is, what the legal violation is. And this is a targeted and streamlined process. Professor Scott Morton, did you have a comment?

Professor SCOTT MORTON. No, I just agree. In particular, if you've got these very specific rules, you're looking for an MFN, discovery is about whether there's an MFN—that doesn't take years. So, I agree with your characterization.

Senator BLUMENTHAL. Thank you.

Ms. LEWIS. If I——

Senator BLUMENTHAL. Professor Francis.

Professor FRANCIS. Senator, I think this is exactly where the rubber meets the road. Right? So, we were told earlier that the harm to competition language in the bill, exactly as you say, in the heart of the cause of action, would make sure that this bill stopped harmful conduct and allowed good conduct. If that's right, then litigation over harm to competition will mean exactly litigation over market definition and market power and effects evidence. It can't be——

Senator BLUMENTHAL. Well, I don't know. You know, if Apple says to an app store, or an app developer, you need to pay 30 percent of your revenue to get on our store and you show the market power of Apple, that's pretty well defined. Right?

Professor FRANCIS. I don't know, Senator. So, number one, I think a lot of businesses charge 30 percent that don't have anything like market power. And number two, I am sure that if there's a harm to competition test in the bill, regardless of where the burden is, there is going to be all the litigation over it that looks exactly like any competitive effects litigation.

Senator BLUMENTHAL. Well, frankly, if my job is to show that Apple has a monopoly or overwhelming market power on app stores, I'll take that side of the case and I won't even charge for it.

[Laughter.]

Senator BLUMENTHAL [continuing]. Thank you, Madam Chair.

Chair KLOBUCHAR. Very good. Thank you, Senator Blumenthal.

So, we have a vote that's been called. I thought I would just ask one more question, and that is actually in the area of hypocrisy, again, with what's been going on around the world. We talked, Ms. Lewis, about how Amazon claimed we'd break Amazon Prime and then, in fact, is agreeing to the exact same thing they said would break Amazon Prime in other countries.

And this Committee has previously heard from small businesses that experienced retaliation. You and I talked about that, and I think that's very important because they've always been emphasizing that they are promoting small businesses, yet we now have many of them that are coming forward, even if they don't want to come forward individually, through their trade associations.

And then on another front, and this involves Apple, we made improvements, as you know, to the bill to clarify that the platforms

can take actions that were reasonably necessary to protect privacy and security. That was something that some of the opponents of the bill—they have about, you know, 15 different things that they try out with Members and test drive, in various ways or send emails about them.

One of them was this, we know they hired some former security people and some of the Members thought they were current security people at one of the hearings. They were not. And, in fact, as I noted, the Justice Department has endorsed this bill.

So, while we heard from Apple that the changes that we made were not enough, they reportedly plan to allow third-party app stores on the iPhone in Europe. Is there any reason why they can't do the same thing in the United States?

Ms. LEWIS. Senator Klobuchar, I am not aware of any reason. And if you look to the example of the fact that a user of a MacBook, or an Apple, a laptop—either their laptops or desktops, are able to download apps from alternative sources and there seems to be no problem with that.

So, I have not heard any credible explanation as to why Apple cannot allow alternative methods of distribution for apps on the iPhone. I see no reason why they can do it in Europe, but they cannot do it here. I see no reason why they can do it for desktops or laptop products, and they can't do it for the iPhone. That just doesn't add up to me.

Chair KLOBUCHAR. Mm-hmm. Exactly. And I think this is one of the failed arguments that they have been trying to make. And we clearly worked with them on making improvements to the bill, but still they persist. So, do you believe that this bill ensures that the companies can continue to protect privacy and security, and even improve their security and privacy provisions if they'd like?

Ms. LEWIS. I do. And so I know that there have been changes to the Open App Markets Act from the version that was introduced in the House.

Chair KLOBUCHAR. Mm-hmm.

Ms. LEWIS. And as you mentioned, many of these changes have been made to respond to criticisms of the bill that it was not sufficiently clear that the covered app stores and the operators would be able to protect user privacy and security.

I think that the bill Sponsors here have gone above and beyond to respond to those criticisms, which I don't think were necessarily valid. I think the bill was—allowed for that in its current form.

But the bill Sponsors have gone above and beyond to add language in response to those critiques, and work with important and knowledgeable civil society groups that are more expert in privacy and security than I am to ensure that the bill does make that clear.

Chair KLOBUCHAR. Mm-hmm. And I think that's the very point. We made over 100 changes to the bill between the introduction, the markup as we headed to the floor. But the point is that they just keep moving the ball. So, they don't really want to work with us on these changes, or they would have, you know, I think, come to some agreement on provisions. But they don't want to. They just want to stop it, and they keep coming up with new arguments. I think that's unfortunate.

Maybe these Section 230 hearings, and the like, will make people be more sensible. But right now, as I noted at the beginning of the hearing, they are just—if we do nothing, we are allowing other countries to come up with the solutions. Some of them we'll like, some of them we won't. But that's what's happening right now.

And it's clear that some of these most common-sense things, that they just hit back at vociferously, are things they actually could do without breaking the internet, breaking Amazon Prime, breaking Google Maps, or breaking the app stores.

So, in any case, this has been an incredibly good hearing. I don't want to be the last one to vote. That would be bad. And I'm really glad one of the benefits of having a year in making over 100 changes and hearing these same arguments over and over again, I think, it's very important for our colleagues.

We had 11 Senators here, which is more than we have for most Full Committee hearings. So people were really able to engage and be part of this discussion, as well as their staffs, either here or watching online. And so that will help to inform them as we go forward, I think, answered a lot of the questions that were raised.

We don't expect to agree on everything, but I am glad, Professor Francis, that we agree on the antitrust funding, and some of the other things that are necessary. And that we all agree that there is a problem, and that we agree that, I would say, just doing nothing may not be the answer here.

So thank you, so much. We're going to leave the record open for 1 week. I imagine some of the Senators that could not join us, or had to leave early, and we really appreciate those that came by, may have some additional questions for the record. And, of course, we welcome that.

So, the record will remain open for 1 week until March 14th, 2023. Thank you, very much. The hearing is adjourned.

[Whereupon, at 5:20 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

A P P E N D I X

Testimony of Adam Candeub
Professor of Law, Michigan State University
Senior Fellow, Center for Renewing America

Senate Judiciary Committee Hearing
Reining in Dominant Digital Platforms: Restoring Competition to Our Digital Markets

March 7, 2023

Big Tech's enormous size and market power pose challenges to the continued vitality of vibrant political discussion in this country as well as democratic deliberation sufficiently robust to hold government accountable to the people. While, as Elon Musk showed America in the Twitter files, Big Tech has focused much of its effort at limiting the ability of all Americans to fully participate in our nation's political discourse.

Consider Big Tech's treatment of Parler. Beginning in 2021, the social media company, which differentiated itself from its competitors by its dedication to free speech and its lack of censorship, held the number one spot on the list of most-downloaded apps on the Apple Play Store. The app was the 10th most downloaded social media app in 2020 with 8.1 million new installs, according to TechCrunch. It was a competitor to incumbent Big Tech platforms, offering consumers a different sort of online experience.

But, then, on vague seemingly pretextual grounds, in early 2021, Apple removed Parler from the App store and soon after Google removed it from the Play Store. Then, Amazon Web terminated its hosting agreement. The Parler app was quite literally "taken down," only returning online months later. It never recovered its business momentum and growth—which are vital for the survival of emerging social media platforms because they depend upon rapidly accelerating network effects. Consumers lost a differentiated social media—and American democracy lost a valuable platform for public debate.

And, sadly, the Parler incident is not a one off. Big Tech appears to be continuing to block many Americans' full participation in political discussion and democratic deliberation. To name just a few recent examples, the RNC is now suing Google over discriminatory email delivery practices that allegedly throttled Republican campaign communications. And, of course, the Twitter files have revealed a long and concerted effort to silence a whole host of often dissenting political views.

The problem of Big Tech stems from its market power. The problem is not simply bias at those companies or a general cultural, moral and political outlook in Silicon Valley that differs dramatically from that of most Americans. Rather, these biases can have massive societal impact because these companies are enormous and dominate internet communications and services.

Firms with significant market power are price givers. They can take actions which may not please some, or even many, of their users without facing competitive challenge or loss of revenue. Their domination of various niches in online business assures them that even if they

decrease the quality of their services, at least as judged by a large segment of America, they will not experience a consequent drop in revenue.

One of the tools of addressing market power is of course antitrust law. And, that presents a dilemma to those like myself who generally stand on the side of economic freedom and business enterprise. But, we must at the same time recognize the challenges that Big Tech poses to fundamental institutions in American society. Many wish to preserve antitrust's productivity, innovation, and allocative efficiency focus. An economics-based consumer welfare standard limits potential bad-effects of a mistaken or overly broad application of antitrust law. But, many cannot close their eyes to Big Tech's deleterious effects on the institutional resilience of our democracy, free speech, children's health and development as well as quite possibly bad effects on economic innovation and growth.

And, this ambivalence comes to the fore when examining how Big Tech's market power allows it to limit the speech of vital voices in our democracy. As the Parler examples shows, a strong culture of free speech requires not simply the First Amendment's formal protections but also demands openness in key avenues and platforms and modes of distribution—such as Google's Play Store or the Apple Store as well as the dominant social media platforms.

Antitrust law has long recognized that special rules could apply when dealing with market power deployed to stifle speech. The Supreme Court's famous statement made in *Associated Press v. United States*, 326 U.S. 1, 20 (1945) makes that point:

"The First Amendment, far from providing an argument against application of the Sherman Act, here provides powerful reasons to the contrary. That Amendment rests on the assumption that the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society. Surely a command that the government itself shall not impede the free flow of ideas does not afford non-governmental combinations a refuge if they impose restraints upon that constitutionally guaranteed freedom. Freedom to publish means freedom for all and not for some." Associated Press v. United States, 326 U.S. 1, 20 (1945)

Similarly, in a different context, the Supreme Court has stated, "assuring that the public has access to a multiplicity of information sources is a governmental purpose of the highest order, for it promotes values central to the First Amendment." Turner Broad. Sys., Inc. v. FCC (Turner I), 512 U.S. 622, 663 (1994).

So, from my perspective—that of concern for the effects of Big Tech on fundamental American institutions such as free speech and the family, I ask whether these bills further a freer country, a stronger democracy as well as a more vital and innovative on-line economy. There is much to admire about these bills, in particular Open App Markets Act But I do have some concerns and suggestions and take the liberty of respectfully sharing them with the committee.

Open App Markets Act

The Open App Markets Act (OAMA) is an admirable effort to combat the power of the large smartphone and internet platforms that host the myriad program and applications we use every day, i.e., mobile apps. Its openness mandates would seem at first to solve the Parler problem. It would seem so, but it's not clear it would. There is no "unreasonable discrimination" provision that prohibits mobile platforms—by which I mean the Apple Store or the Google Play Store—from making arbitrary or discriminatory exclusion of apps from their platforms. Rather, there is a requirement in Section 3(a)(2) that would prohibit a mobile platform from offering prices or terms and conditions worse than any other platform—which does not address the problem directly.

But, even if that provision would solve the problem, which I'm not sure it would, Section 4 has a rather extensive set of exceptions, allowing covered platforms to exclude firms if "necessary to achieve . . . digital safety." Section 4(a)(1)(A).

What is "digital safety"? Make sure you don't take a bath with your iPhone lest you get electrocuted? As a law professor who specializes in communications law, I confess I never heard of the term until I read it in the bill. But, a little research reveals that it is indeed a concept with an accepted meaning—and, interestingly, it is a concept strongly pushed by, and perhaps even coined, by the World Economic Forum.

The World Economic Forum has, in fact, a Global Coalition for Digital Safety that "aims to accelerate public-private cooperation to tackle harmful content online and will serve to exchange best practices for new online safety regulation, take coordinated action to reduce the risk of online harms, and drive forward collaboration on programs to enhance digital media literacy."[1]

Of course, trying to figure out how the World Economic Forum defines "harmful content" or perhaps we should say "digitally unsafe," content is not an easy matter. The WEF never defines it explicitly. But, sifting through their documents, written in vague bureaucratic language, we find a white paper from June 2021, "Advancing Digital Safety: A Framework to Align Global Action."[2] Here we learn that "in the United States, for example, these private companies are not obligated to protect First Amendment speech rights and can moderate certain categories of harmful but legal ("lawful but awful") content."[3]

Or we can look to the policies of the large tech companies themselves. Apple's app developer guidelines, requirements that apps censor "discriminatory, or mean-spirited content," are under the "Safety" guidelines.[4]

So, it would seem as if this section would allow for the censorship of apps or other material that would be "lawful but awful." As the Twitter files unequivocally show, the employees of the

[1] World Economic Forum, https://initiatives.weforum.org/global-coalition-for-digital-safety/home.
[2] World Economic Forum, White Paper, *Advancing Digital Safety: A Framework to Align Global Action* (June 2021).
[3] *Id.* at 7.
[4] Apple Developer Guidelines, https://developer.apple.com/app-store/review/guidelines/#user-generated-content.

major platforms have notions of what constitute "awful" that align more closely with the Davos crowd than with American traditions of free expressions.

As written and in practice, therefore, I fear the current wording without a general viewpoint antidiscrimination provision would not solve the Parler problem. There is a large loophole—a loophole through which Apple, Google, and Amazon would be able to kick out Parler or anyone else for that matter.

American Innovation and Choice Online Act

The American Innovation and Choice Online Act (AICOA) is a far more expansive and comprehensive bill. It's primary operative provision, Section 3, contains a list of ten prohibited practices that go beyond what is currently prohibited under antitrust law. It is not exactly clear how they will apply and what they prohibit so that the act explicitly empowers the DOJ and FTC to interpret them so as to make sense for the platforms.

Even as one who shares many conservatives' ambivalence toward Big Tech, the prohibitions give me pause. And, I suspect my fellow witnesses today will provide an economic critique far more incisive than any I could offer. I will only say that these prohibitions go far beyond what current antitrust law provides, include very difficult and vague standards, and may not achieve the goals of significantly weakening Big Tech. Furthermore, it won't solve the problem of Parler and unfair discrimination by the platforms, a concern of many Americans.

On the other hand, given that their prohibitions are focused on, at least on the consumer side, a handful of firms, i.e., those with over 50,000,000 users, any deleterious inefficiencies will not be visited on the entire economy but concentrated in a few firms. Further, we must ask ourselves whether these firms actually increase consumer surplus. Some—but certainly not all—of the affected firms are large social media companies. They provide free services—and any consumer surplus must be inferred through often complex economic calculations. This is opposed to normal goods which have prices that indicate value. As research has shown, however, many of these services have a negative hedonic effect, i.e., using social media seems to make us unhappier. And, the value users place on social media is time-inconsistent, not unlike addictive substances.[5] This may result in over estimation of the value of social media—and indeed an indeterminacy in all economic claims about social media's benefit.

Further, the macro-effects of social media, as many leading psychologists have concluded, have been horrible for young people, particularly adolescent girls and young women, who face epidemic levels of loneliness and mental illness.[6] A recent CDC report sadly documents the frighteningly bad mental state of American youth.[7] Typical economic analysis has difficulty

---

[5] Allcott, H., Braghieri, L., Eichmeyer, S., & Gentzkow, M., *The welfare effects of social media*. 110 AMERICAN ECONOMIC REVIEW 629-67 (2020).

[6] Twenge, J. M., Haidt, J., Blake, A. B., et al., "Worldwide increases in adolescent loneliness." Journal of Adolescence 93 (2019); Hunt, M. G., Marx, R., Lipson, C., & Young, J., *No more FOMO: Limiting social media decreases loneliness and depression*, *37* J. SOCIAL AND CLINICAL PSYCHOLOGY, 751-768 (2018).

[7] Center for Disease Control, Youth Risk Behavior Survey 2011-2021 (Feb. 2022).

grappling with these effects. But, these effects do lessen the concerns about law-induced inefficiencies in the provision of social media.

Yet, even with these caveats, the American Innovation and Choice Online Act may simply be ineffective—particularly at promoting free speech. Indeed, it might produce the opposite. And, that's because of its enforcement mechanism. There is no private action. It's a very big stick that DOJ, the FTC, and the state attorney generals can use to hit Big Tech.

As the Twitter files reveal, government's power over the Big Tech can have bad effects on free speech. In today's information economy a few platforms have enormous power over public and private conversation, professional journalism and citizen debate and engagement. As we have seen, government can too easily apply pressure to have the platforms silence speech it doesn't like. The American Innovation and Choice Online Act, with its vague terms and discretionary and exclusive governmental enforcement, simply adds to the available pressure government can employ on the major internet platforms to silence government's critics.

Written Questions of Senator Grassley for Adam Candeub, U.S. Senate Judiciary Committee, Antitrust Subcommittee Hearing "Reining in Dominant Digital Platforms: Restoring Competition to Our Digital Markets," March 7, 2023

Questions for Adam Candeub

I'm very concerned with the government's ability to engage with platforms to silence speech. I've been working with Senator Lee on a bill which would protect users of online platforms from censorship. Do you believe that Senator Lee's legislation would help to more directly address this censorship problem?

I do not believe that Senator Lee's bill has been released yet. I look forward to reviewing it and would be delighted to share my views with you or your staff when I do so.

Questions from Senator Tillis
for Adam Candeub
Witness for the Senate Committee on the Judiciary Subcommittee on Competition Policy, Antitrust, and Consumer Rights Hearing "Reining in Dominant Digital Platforms: Restoring Competition to our Digital Markets"

1. What are the legitimate privacy and security concerns that could be created by the Open App Markets Act and the American Innovation and Choice Online Act? Based on these concerns, what further recommendations do you have to improve this legislation to ensure it adequately protects user privacy and security?

   Many have raised with the Committee privacy and security concerns. Some claim that in order to introduce new and enhanced privacy or security protections under the bills' legal requirements, a mobile platform would have to prove the protections were "necessary" and "narrowly tailored" as well as that no less restrictive protections were available. Parties claim that this test is too burdensome. Further, the bills would allow "sideloading," the process of direct installation of software from the internet that circumvents platforms' privacy and security protections. This would allow predators and scammers to sidestep platforms' privacy and security protections—and take from consumers the option of choosing a platform protected from malicious and dangerous code.

   Others take a different view. They note that other platforms, such as Android, allow sideloading, and that consumers seem happy with that platform. Further, the bills do not require one-click installation of random apps from the Internet, only that companies relinquish their monopoly control over app stores, allowing other stores to provide apps. These stores could have the same, or even additional, privacy and security restrictions than those the platforms now use. Thus, the bills could give consumers more choice. And, of course, users would be under no obligation to use any app store other than that provided by the device manufacturer.

   In the end, this debate centers around consumers' control of their internet experience and their devices. There indeed may be a tradeoff between openness and security, but consumers should have the information that allows them to make the best choices and figure out their own appropriate tradeoffs. The bill's privacy and security section could, therefore, be strengthened by including greater transparency requirements to better disclose platform's privacy and security measures.

2. What does the Open App Markets Act and the American Innovation and Choice Online Act do to affirmatively protect user privacy and security if platforms are required to adopt certain practices? Is this enough to prevent misuse from bad actors? Should these proposals do more to mitigate bad actors?

   The Open App Markets Act allows platforms to adopt the privacy and security practices that they believe best serve their consumers' interests and demands. Requiring devices to host multiple app distributors does present additional concerns about privacy and security. But, it is difficult for the government to prescribe technical standards—and perhaps it shouldn't absent a more compelling and detailed legislative record. Again, allowing individuals to make their own decisions about privacy and security—through added disclosure and transparency requirements about platforms' privacy and security measures—may be warranted to both deter bad actors and allow individuals the uses they want.

3. For the Open App Markets Act and the American Innovation and Choice Online Act what is your view of the definition of the terms "covered company" and "covered platform," respectively, in these proposals? What are your thoughts about the thresholds used to define the terms "covered company" and "covered platform?"

   Determining size thresholds for a law's applicability always presents a problem requiring careful legislative judgment. Certainly, the definitions that are currently used would include those firms about which many Americans have concerns.

4. For the Open App Markets Act and the American Innovation and Choice Online Act do the terms "covered company" and "covered platform" strike the appropriate balance of regulating entities most responsible for the respective conduct at issue? Are there any other amendments that you would make to the definition of "covered company" and "covered platform," and if so, what amendments would you make?

Determining size thresholds for a law's applicability always presents a difficult legislative decision. Certainly, the definitions that are currently used would include those firms about which many Americans have concerns. I am not in a position to offer an opinion on the precise threshold that "strike[s] the appropriate balance of regulating entities most responsible for the respective conduct at issue."

5. Ensuring user privacy is extremely important to me, and consumers should have transparency about how their data is being used. User data is valuable in large part because it helps private businesses tailor services and goods to their customers in ways customers find helpful. Does the Open App Markets Act and the American Innovation and Choice Online Act strike the appropriate balance between ensuring consumer control of their data and permitting appropriate use of data by the platform?

Privacy is always a tradeoff. The greater openness a platform or service provides, the greater access to other people or entities, the greater possibility that data will be inappropriately obtained, retained, used, or shared. At the same time, sharing data allows for online firms to provide goods and services that best match consumers' demands.

The question is who is best suited to determine the appropriate level of risk in sharing data—and thereby determine the balance between privacy and efficiency. Under free market principles, consumers are best able to determine appropriate use of their data. If the bills are strengthened to include further disclosure about privacy and security practices, consumers will be able to choose app stores that best match their preferences as far as consumer data use and privacy.

6. In your opinion is it better to consider the sort of wholesale comprehensive revisions to existing antitrust law or more targeted and precise reforms?

That is difficult question to answer, and I think the best answer is that "it depends." Given the systemic effect of wholesale comprehensive revisions to existing antitrust, such efforts should not be undertaken unless there is considerable concern about increasing concentration throughout the economy. And, some economists do have that concern. On the other hand, antitrust law is slow to work and often cannot keep up with technological change. Digital markets change so rapidly that the data required for a court to establish market definition and other factual findings in antitrust litigation often do not exist. Under such circumstances, targeted approaches, which have less risk for unintended consequences, may be wiser.

7. In your opinion does the Open App Markets Act or the American Innovation and Choice Online Act threaten to negatively impact U.S. innovation is any way? And if so, how?

There is always the argument that mandating access to a private firm's platform, network, or other type of facility could decrease dynamic efficiency. A firm will not build platforms if government mandates such firm to provide access to competitors. On the other hand, making essential inputs, such as distribution of online applications, to all may increase innovation by lowering the cost of distribution to startup firms.

To riff on Yogi Berra, "It's tough to make predictions, especially about the innovation." Unlike antitrust and allocative efficiency, there are no precise economic models for how and when companies and economies innovate. Common sense must guide policy-makers.

8. NSA, NIST, DHS, FTC, and other federal agencies have raised concerns about sideloading, and recommend consumers only download apps from the store provided by the device manufacturer or operating system

provider. Do you share these concerns – why or why not? How should we evaluate these proposals in light of the concerns raised by federal agencies?

I do share these concerns. It is my understanding of the bills, however, that they do not require one-click installation of random apps from the Internet, only that companies relinquish their monopoly control over app stores, allowing other stores to provide apps. These stores could have the same, or even greater, privacy and security protection than that which the major platforms now provide. I think many of the agencies' concerns could be remedied through greater transparency and disclosure concerning platforms' privacy and security functions. Such disclosures could allow consumers to make the best choices of which app stores to use for themselves and their families.

WRITTEN TESTIMONY OF

DANIEL FRANCIS

ASSISTANT PROFESSOR OF LAW

NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE U.S. SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS

FOR A HEARING ENTITLED

"REINING IN DOMINANT DIGITAL PLATFORMS: RESTORING COMPETITION TO OUR DIGITAL MARKETS"

MARCH 7, 2023

TABLE OF CONTENTS

I. INTRODUCTION AND EXECUTIVE SUMMARY

Chair Klobuchar, Ranking Member Lee, Members of the Subcommittee, thank you for the opportunity to appear before you today. My name is Daniel Francis. I am an Assistant Professor of Law at NYU School of Law, where I teach and write about antitrust. My academic work currently focuses on ways to reinforce our antitrust laws, in digital and other markets, without sacrificing principle or rigor.[1] I am also a former federal antitrust enforcer: from May 2018 to January 2021, I served in the antitrust arm of the FTC as Senior Counsel, Associate Director for Digital Markets, and ultimately Deputy Director. My work at the FTC focused on digital and platform antitrust, including among other things the Facebook (now Meta) monopolization investigation and litigation, which challenged the acquisitions of Instagram and WhatsApp as well as the application of certain platform policies. Before joining the FTC, I spent a little more than ten years in private practice.

I do not work for or represent any private clients, and I have not done so since joining the FTC in May 2018. I have no brief in testifying today other than my interest in protecting consumers and supporting the antitrust system, particularly in digital markets.

I strongly support vigorous antitrust enforcement, including in digital, platform, and high-technology markets. In particular, I support: (1) significantly increasing the funding and staffing of our antitrust agencies, which have fallen far off the pace (for example, from FY 1979 to FY 2021, the volume of HSR merger filings has increased to more than *four times* what it was in

[1] *See, e.g.*, Daniel Francis, *Making Sense of Monopolization: Antitrust and the Digital Economy*, 84 Antitrust L.J 779 (2022) (proposing a principled reinforcement of monopolization law); Steven C. Salop, Daniel Francis, Lauren Sillman, and Michaela Spero, *Rebuilding Platform Antitrust: Moving on from* Ohio v. American Express, 84 Antitrust L.J. 883 (2022) (proposing a balanced approach to platform antitrust after *AmEx*); Daniel Francis, *Revisiting the Merger Guidelines: Protecting an Enforcement Asset*, Comp. Pol'y Intl. (Nov. 2022) (proposing protection of the guidelines' status as a trusted enforcement tool).

FY 1979, while the FTC's full-time-equivalent ("FTE") staffing utilization declined by more than a third over the same period[2]); (2) increasing support for state antitrust enforcement; and (3) reinforcing our core antitrust statutes to restore vigor and reduce ambiguity, and adding merger review time for the most troubling deals, to save agencies and businesses from kneejerk decisions.

I would also support (4) some regulation of digital platform markets, *if targeted to specific practices and in the interests of consumers*. This could include, among other things: (a) transparency and disclosure obligations in ad-tech markets; (b) consumer transparency obligations to require disclosure of paid advertising that resulted in improved search rankings or preferred placement; (c) a targeted ban on the use of most-favored-nation ("MFN") clauses by digital platforms with significant market or monopoly power, in markets in which the harms from MFNs would generally outweigh their benefits; and (d) market-specific interoperability or portability obligations for businesses with significant market or monopoly power, targeted at markets in which such obligations could be reasonably defined and enforced, and subject to robust defenses to protect consumers, businesses, and platforms.

But I do not recommend enacting AICOA, nor do I recommend enacting OAMA in its current form. In summary, my views are as follows.

A. AICOA

I think AICOA pursues an important and valuable goal—competition in digital markets—but it does so in the wrong way, and at much too high a price for American consumers. The bill centrally demands that our economy's largest platforms should do *less* for consumers and *more*

[2] Even with recent funding increases, projected FTC staffing for FY 2023 will be around 83% of FY 1979 FTE utilization. *See infra* § IV.A.

for other businesses. In the process, I think AICOA will end up deterring beneficial practices and business models, giving a helping hand to bad actors, and triggering a generational landslide of confusion and costs. It aims at Big Tech, but it will hit consumers, and I do not think its uncertain benefits justify its evident costs and risks.

I also fear the broader implications of regulation so obviously aimed at a set of particular businesses. AICOA targets some politically unsuccessful, but very different, businesses for a unique, uniform package of regulatory burdens disconnected from market power tests. Congress has historically refrained from using antitrust or competition policy to pick individual winners and losers in our economy. I deeply fear the present and future costs of leaving that path.

The heart of AICOA is a prohibition against "self-preferencing." But a ban on self-preferencing would prohibit or deter an array of valuable practices that benefit consumers, including through product improvements, feature innovations, new market entry, and low prices. "Self-preferencing" as AICOA defines it includes a host of product improvements that are clearly desirable: adding a Google Maps widget in a Google Search results page; preinstalling Apple Maps on an iPhone; including Microsoft applications with Microsoft Windows; making Prime Video available for free to Amazon Prime subscribers; promoting in-house content on Apple+ and Prime Video; and so on. I cannot imagine why we would want to define an offense that includes such practices! Platforms should be free to improve, integrate, distribute, add, and promote features, products, and services—even when they cannot or would not do so, or would do so less, under a forced-sharing regime covering a limitless array of third parties.

AICOA threatens other harms too. Under AICOA, covered platforms will live under the dangling sword of lengthy investigations and litigations: including the threat of disruptive interim

injunctive relief, which AICOA makes available on a specially lowered threshold, and the prospect that responsible executives will personally have to forfeit their compensation. As a result, platforms will be deterred from protecting consumers by denying access, preinstallation, distribution, and so on to third-party businesses, *even when the platform has reasonable grounds for concern.* Those grounds might be, for example, that an app or product might be buggy or badly interoperable with the platform; low-quality; spammy; objectionable in content (*e.g.*, sexually explicit material or the promotion of terrorism and violence); malicious; controlled or influenced by or vulnerable to a hostile power; very costly to integrate; and so on.

This deterrent effect will bite in cases where AICOA's narrow affirmative defense does not apply—it does not cover most of the grounds just described—as well as in cases where the platform could not or does not want to go fifteen rounds with the FTC to defend the decision, nor to run the risk of a massive fine and an injunction. Forcing executives to bet their own compensation when they say "no" instead of "yes" to a third party magnifies the problem.

Of course, some of those close and borderline cases will involve good actors and great products that will obtain platform access as a result of AICOA. That will certainly be a benefit. But more bad actors will still get through the door, even if the changes are made at the behest of, and in hope of helping, legitimate competitors! I do not think there is much room to doubt that AICOA will result in more bad actors and more bad products—ranging from the malicious and sinister to the merely buggy and spammy—getting access to platforms, data, consumers, devices, and ecosystems. As the Internet of Things expands and more devices go online, this means more bad actors getting easier access to consumers' lives and homes.

I think this is too high a cost. There are plenty of hostile and malicious actors in the world today searching constantly for new ways to access consumers' devices, data, and homes. And it seems a particularly bad time to make our critical digital infrastructure more vulnerable by deterring our most important platforms from protecting their own systems and users. Platform decision-makers should not be given a choice of *either* letting suspicious third-party apps and entities into their ecosystems *or* facing the threat of complaints, investigations, litigations, injunctions, and penalties (and the forfeiture of their personal compensation!).

As I read it, AICOA also presents a sharp challenge to two business models that are associated with real consumer benefit. First, it threatens the operation of free-to-use, ad-supported businesses, where the provision of free services is made possible by preferencing the platform owner's own advertising, or a service that carries it. Deterring businesses from using that model—and driving them toward fee-paying models—does not seem likely to benefit consumers overall. Second, it also threatens closed or partly closed systems which offer users and businesses a secure, seamless option. But cybersecurity experts overwhelmingly emphasize the safety benefits of closed systems, and of platform-owners' power to restrict and deny access to third party code.

I do not think AICOA's qualifying provisions—a harm to competition test and two affirmative defenses—do much to save the legislation. As others have pointed out, AICOA doesn't explain whether this "harm to competition" test is supposed to be a consumer welfare test, an injury-to-rivals test, or something else, nor even whether it is intended to be construed consistently with antitrust jurisprudence. "Competition" does not, alas, have a single obvious meaning. Strategic ambiguity on this point in legislation of this scale and novelty seems highly undesirable.

And in forced sharing cases, I think the "harm to competition" test will be a dead letter in practice. Forced sharing virtually always seems good for competition *after an improvement has already been created*—why not make an already-created benefit widely available?—despite the harm to *future* investments and improvements that will be done by such a mandate. If the intention is to permit any self-preferencing that is reasonably related to incentivizing a procompetitive investment, AICOA should say so—but, of course, this would dramatically narrow the bill.

AICOA's general affirmative defense is too narrow and too demanding to offer much comfort. It does not protect, for example, denials of equal treatment based on: objectionable content (*e.g.*, sexually explicit content, promotion of terrorism or violence); false information; poor quality service; spam; fraud; consumer confusion; threat to the security of other ecosystem participants; and technological, commercial, or other difficulties and costs of integration. The product improvement defense is limited to improvements of "core" functionality (an utterly critical term that is inexplicably left undefined). And even a product improvement is unlawful if its objective "could be achieved" on a non-discriminatory basis: regardless of whether a rational or reasonable platform would be willing in practice to incur the necessary burdens, or whether it would be profitable to do so. And, in any event, a fact-specific defense—that a platform might or might not be able to prove to the satisfaction of an agency or court after months or years of expensive, disruptive investigation (perhaps with interim relief freezing its business in the process, and with penalties and injunctions hanging overhead, *and* with the decision-maker's personal compensation on the line!)—is going to be cold comfort to a platform in practice.

I wonder whether Congress might be centrally concerned with a *much* more specific problem: intentional, targeted, and unjustified discrimination against rivals of the platform

monopoly itself. Here the concern would *not* be that the platform is improving its own product while not doing so for third parties: the concern would be that the platform generally supplies something to the world already (whether or not it treats itself even better), and targets particular rivals for discrimination simply to forestall competition in the platform's own primary market. If this is indeed Congress's concern, it is a *much* narrower phenomenon than the broad array of conduct reached by AICOA. It could be addressed with a single short prohibition that would avoid most of the costs and harms that the existing draft threatens. There are, to be sure, reasons why Congress might not want to go even that far—it is after all not obvious that businesses, even big ones, should always have an affirmative obligation to subsidize and support their rivals—but a narrow ban on intentional, targeted, and unjustified discrimination against rivals of the platform monopoly would be *vastly* less harmful to consumers than the current version.

One final comment. By making existing digital platforms more comfortable for suppliers of complementary products and services—through extensive entitlements to certain kinds of access and favorable treatment—AICOA perversely *suppresses* incentives for competition against the platforms themselves. When the federal government forces a monopolist to treat me better, I become less interested in competing with it or supporting entrants or rivals (from whom I get no such special treatment). AICOA thus tends to perpetuate the dominance of covered platforms, turning would-be disrupters into cosy stakeholders in the status quo, while *also* restraining platforms' own competitive vigor. This seems to have everything backwards.

To sum up: AICOA is built on two premises—that self-preferencing is nearly always harmful, and that a general equal-treatment obligation is better for consumers—and I think each of them is wrong. Platforms should not be penalized for better serving consumers, even when they

cannot, would not, or should not serve other businesses on equal terms, or at all. Competition protected by antitrust, not monopoly entrenched and sedated by regulation, should be our goal.

B. OAMA

I think OAMA provides a better model, with respect to both scope and substance, for digital platform regulation than AICOA. I would support a version of OAMA that was limited to more targeted versions of some of its provisions, and that was supported by more robust defenses for platform conduct that protected consumers, business users, or the platform. But I do not support the bill in its current form.

The positives first. There is plenty to like in OAMA's basic design, including above all its specificity and granularity. OAMA is focused on two specific and reasonably well-defined set of markets that are important to digital competition, in which we might plausibly have a fairly consistent set of concerns. Namely: (1) markets for the sale and distribution of apps; and (2) markets for the provision of app-store services. OAMA seems unlikely to prohibit a wide range of product improvements and innovations. And it clearly reflects some effort to allow platforms to take reasonable measures for good reasons.

On substance, I also would support more targeted versions of some of OAMA's provisions:

- **App pricing MFN ban for app stores with significant market / monopoly power.** I would support a carefully targeted ban on the use of app pricing most-favored-nation ("MFN") clauses by app stores with significant market or monopoly power. Although these commitments can enable better pricing, they can also deter discounting by developers to other channels as a means of encouraging inter-platform competition. For example, if apps become cheaper on one platform than on another, the second platform may come under

competitive pressure to improve its own pricing. Or if a major app developer wants to support and sponsor a new entrant, it may discount to bring that entrant into the market. But an MFN commitment forces developers to share any such discounts with all MFN beneficiaries, thus making discounting more costly and less attractive. And an MFN that benefits an incumbent with market or monopoly power will prevent a developer from discounting to spur some competition against that incumbent.

- **Limited non-use obligation for competitively sensitive nonpublic information, for app stores with significant market / monopoly power.** I would cautiously support a limited ban on an app store's competitive use of competitively sensitive nonpublic business information received directly from the app developer as a condition of operating an app store, for app stores with significant market or monopoly power. As I explain below, I think the non-use obligation in the current draft is much too broad and would harm consumers. Just like supermarkets and other businesses, app stores should be able to use data generated by the store to improve its own products, even in competition with developers. They should also be able to buy and sell data in order to improve their own products and services. But one could reasonably fear that an app store might require developers to supply competitively sensitive nonpublic business information (such as app code, or advance notice of planned features) as a condition of participation on a store, in ways that would eliminate or erode developers' own incentives to invest in apps and app improvements. I am not sure that there is evidence this is a serious problem in practice, but a rule against it might do some good now or in future.

- **Disclosure obligation for preferred-placement advertising.** I would support a disclosure obligation that required app stores to disclose preferred placement in search results or rankings as a result of paid advertising. This would benefit consumers and harm no-one.

But I do not support the rest of OAMA. Most importantly, I fear that forcing covered companies to host third party app stores and in-app payment systems would compromise security and quality in ways that would expose consumers and others to serious harms and dangers. Cybersecurity experts *overwhelmingly* emphasize the dangers of third party app stores and of malicious apps. It is clear that official app stores, empowered with the ability and incentive to guard against hostile code and bad actors of all kinds, are the best hope of defending consumers from a proliferating array of threats. I think it would be a terrible cybersecurity mistake to breach these defenses and give third party app stores, and third party apps, a new weapon to force their way into digital ecosystems. In addition, I would apply a significant market or monopoly power test as a prerequisite for any obligations aimed at protection against competitive harms.

Finally, I also recommend limiting OAMA's enforcement to government authorities. Private enforcement—with the threat of treble damages, injunctive relief, and class actions—increases the risk that OAMA will be used in ways that do not serve the public interest.

*

The remainder of my written testimony is structured as follows: Part II addresses AICOA; Part III OAMA; and Part IV offers an alternative roadmap for supporting competition throughout the economy, including vigorous antitrust enforcement as well as some carefully targeted platform regulation.

II. THE AMERICAN INNOVATION AND CHOICE ONLINE ACT (S. 2992)

I have reviewed a draft of the American Innovation and Choice Online Act ("AICOA"), S. 2992, as reported to the Senate on March 2, 2022, and as further amended in a draft published by Senator Klobuchar, the bill's sponsor, on May 25, 2022.[3] For the reasons explained below, I do not recommend enacting AICOA.

A. Summary

The strongest case for AICOA, as I understand it, depends on two related claims. The first claim is that *platform self-preferencing is generally bad for consumers*. The second claim is that *a ban on self-preferencing would be better for consumers than the status quo*. I do not recommend enacting AICOA because I believe each of those claims is wrong. And I expect that enacting AICOA would harm consumers overall, not help them.

I believe that the first claim is wrong because "self-preferencing" includes a vast array of product improvements, feature innovations, and other practices (including those supporting new entry) that American consumers value enormously. Platform self-preferencing includes many familiar and beneficial practices, including for example: the integration of Google Maps information into Google Search results; the preinstallation of Apple apps on iOS devices; the preinstallation of Microsoft software on Windows computers; the special promotion on the Amazon and Apple+ platforms of their own in-house content; and the closer integration of in-house virtual assistants with platforms or in-house apps with virtual assistants.

---

[3] Draft available here: https://www.klobuchar.senate.gov/public/_cache/files/b/9/b90b9806-cecf-4796-89fb-561e5322531c/B1F51354E81BEFF3EB96956A7A5E1D6A.sil22713.pdf ("AICOA (May 2022 draft)"). In focusing on the May 25, 2022, draft, I follow the Congressional Research Service. Congressional Research Service, *The American Innovation and Choice Online Act* (Aug. 30, 2022); *see also* https://www.congress.gov/117/bills/s2992/BILLS-117s2992rs.pdf (version as reported May 2, 2022).

These and similar practices are good for consumers, even if the platform in question has market or monopoly power. Sometimes these practices will help to improve the interoperation of two existing products, services, or businesses; sometimes they will involve giving consumers additional benefits; sometimes they will play an important role in incentivizing and supporting entry by platform businesses into new markets. (For example, Apple's incentive to invest in creating and supporting Apple+ content, or Amazon's incentive to invest in creating and supporting Amazon Studios content, was clearly augmented by the opportunities for promotion on their respective platforms.) Indeed, *any* practice by an integrated business that makes products and services work better together is "self-preferencing" unless the business also makes the same improvement available to every other third-party business. It is routine throughout our economy, and I do not think Congress should legislate from the premise that it is a presumptive problem, either in general or in digital markets.

And I believe that the second claim is wrong because a ban on self-preferencing would actively harm consumers, in addition to whatever good it might do. I predict at least five separate kinds of harm. *First*, I expect that the ban would deter improvements and other practices that consumers value, including the practices described above. By telling platforms that they may not implement a product improvement unless they are able and willing to extend it to a limitless class of third parties seeking equal treatment, AICOA would lead to fewer new improvements, withdrawal of existing ones, and resulting consumer harm.

Second, I expect that the ban would deter platforms from protecting consumers, businesses, platforms, and even national security, in close or borderline cases. Under AICOA, denying third-party demands for equal treatment (preinstallation, high search ranking, access to consumer data,

etc.) threatens complaints, investigations, litigations, penalties, injunctions, and the personal forfeiture of compensation. At the *very* least this means significant costs, delays, and uncertainty. Platforms will therefore face an incentive to give in to third-party demands, and grant third parties access on equal terms, *even in cases where there are genuine grounds for concern*, if the platform fears that it may not ultimately be able to prove those grounds, or where the burdens and costs of trying to do so may be significant. (Or where a decisionmaker is just very risk-averse when it comes to putting his or her own salary on the line!) As a result, more bad actors will get access to platforms, consumers, and data. At a time when there is no shortage of hostile and malicious actors in the world seeking to harm the United States and its citizens, it is an odd time to encourage our most important platforms to lower their guard.

Third, I expect that the ban would threaten the provision of ad-supported business models, many of which involve providing free or low-cost services to millions of Americans through a business model that promotes a platform's own advertising channel. Prohibiting platforms from apps and functions that support those ad services (or even the ad services themselves, depending on the definition of "business user"[4]) strikes at the heart of the underlying business model that makes such free service possible. And if the result is to drive digital businesses to migrate from free-to-use, ad-supported business models to fee-based models, I fear that millions of Americans will pay more, and get less, than they do today. Free access to digital services is a critical tool for giving American families access to knowledge and opportunity. I think it would be unwise to make that model a losing proposition for our most critical digital businesses.

---

[4] *See infra* note 11.

Fourth, on the most natural reading, I expect that the bill would be read to prohibit or deter "closed systems" in which a business opts to run its system, in whole or part, without third-party participation.[5] Closed systems, or parts of systems, are common in the digital economy. For example, Apple does not allow third-party device manufacturers to participate in its iOS system, and Amazon does not allow third-party music streaming platforms to participate in its Amazon Prime ecosystem. (Outside the world of the covered platforms, it is also common: for example Disney does not generally allow third party content creators to participate in its Disney+ platform, and so on.) Closed systems are overwhelmingly associated with a more secure and more seamless experience for users. Banning that business model seems unwise and harmful.

Fifth, I expect that AICOA would perversely suppress interplatform competition—that is, competition *against* covered platforms in the market in which the "main" platform itself competes—in an effort to support competition *on* covered platforms. Trading partners that are given special benefits on a covered platform have less incentive to create, invest in, or sponsor, competitors of the platform. Instead, they become comfortable stakeholders in the status quo. I appreciate that some might conclude that the current generation of covered platforms will never be displaced, and are therefore happy to make that trade. I do not share that confidence. I think entrenching and perpetuating existing incumbency, and hoping to manage the results, is a mistake.

To be sure, there will be some benefits. AICOA would have some effect in favoring third parties over incumbent platforms in "secondary" markets where platforms also compete, and some third parties will do better as a result. Consumers may or may not benefit from that effect. But I fear that this uncertain benefit would come at much too high a cost. Moreover, to the extent that

[5] *See infra* note 11.

Congress's concern is really with intentional, targeted, and unjustified discrimination by dominant platforms against actual or potential rivals (*e.g.*, an effort to deny rivals access to complementary markets as a means of protecting the platform monopoly), a narrow rule could address that concern with *much* less collateral harm.

The "harm to competition" test in the current draft of AICOA does not much reduce my concerns. For one thing, it is not clear whether it contemplates a "consumer welfare" test drawn from traditional antitrust, or an "injury to rivals" test reflecting AICOA's separate nature and purpose. It cannot be both. This point is too important to leave intentionally unresolved.

Even a welfare-based test does not seem likely to help platforms in forced sharing cases. The harm to competition test, as I read it, invites a court to compare a world with forced sharing against the status quo. But that *ex post* test will *always* tend to find that forced sharing would improve competition compared to no sharing. The harm to competition test will thus become a rubber stamp. This implicates a classic fallacy in the analysis of refusals to deal. Suppose, for example, that a business spends five years and $10 billion to develop a valuable active pharmaceutical ingredient, or technology, over which it obtains a patent. If we come along *after the investment has been made* and ask whether it would improve competition to forcibly share the active pharmaceutical ingredient or technology with rivals, the answer will invariably be yes. More output and lower prices is better than less output and higher prices! So the apparent conclusion is that forced sharing of the asset is good for competition. But the fallacy arises from failing to think about the *ex ante* perspective: that is, the impact of a forced-sharing rule on the decision to invest in the first place. When we impose such a rule, we drain the incentive to invest, with the result that the ingredient or the technology may never be invented in the first place.

I fear just such an effect here. The point is not that *no* innovations will arise: it is that there will be *less* investment and innovation by some of our most important businesses. A forced-sharing rule makes it much less appealing to invest in things that are covered by the rule, so businesses are more likely to do something else with their time and money instead.

Nor do the affirmative defenses allay my concerns. Some important policy justifications are omitted entirely. For example: AICOA does not allow platforms to deny equal treatment to third parties, or their products and services, because they: are buggy or badly interoperable with the platform; are of low quality; contain objectionable content (*e.g.*, sexually explicit content, promotion of terrorism or violence); contain false or inaccurate information; promote spam; constitute or facilitate fraud; are subject to control or influence by, or are vulnerable to, a hostile or malicious entity; or because integration would present unusual technological or other commercial difficulties, or costs.

Remarkably, even product improvements are allowed *only if* they relate to "core" functions (an undefined term!) *and, further, only if* the platform can show that it "could not" achieve the improvement in a less discriminatory way. A platform does not seem to have the option of saying: "OK, it would be technically possible, but no rational platform would go to the trouble and expense of sharing this improvement with all third parties. We would rather not implement it at all than take on that burden, which would wipe out the profit case for doing it in the first place. The whole point of our investment was to make *our* product more valuable, not to subsidize competitors."

Finally: the difficulties and burdens of proving up a fact-heavy defense, with an array of burdens and penalties hanging overhead, will seriously erode the utility of the defense in practice.

*

To be sure: anticompetitive practices and transactions present a serious threat in digital markets, just as they do in other markets that matter to American consumers and workers. But to deter digital platforms, from engaging—*not* in improper collusion, anticompetitive acquisitions, and so on, but *product improvements, feature innovations, and entry*—has it entirely backwards. This kind of thing is exactly what we are spending millions of antitrust enforcement dollars with our left hand in an effort to get platforms to do: compete on the merits by providing valuable combinations of high-quality products and services to consumers for low prices. We should not bash them for it with our right hand when they do so.

Three final general comments. First, the scope of AICOA is exceedingly puzzling. There are serious and profound differences between the business models of the covered platforms, and each covered platform is active in a wide variety of markets. Competitive conditions, and competitive concerns, differ widely across those countless markets. I cannot discern any neutral rationale for including these businesses with respect to all their business lines and excluding other businesses, including other large monopolists, in a single regulatory measure like this one. This approach may give rise to the appearance that these businesses are being singled out not because of any distinctive competition-policy problem (there is plenty of monopoly power, network effects, data, and vertical integration throughout the rest of the economy) but because of political unpopularity. It also runs the twin risks of: (1) "fighting the last war," by focusing on a set of businesses that have already achieved some kind of dominance, rather than relying on antitrust to protect competition with the next wave of digital businesses and across the economy; and, ironically, (2) cementing the position of AICOA's covered platforms, by softening the incentives of other businesses to create or support alternatives.

Second, antitrust enforcement experience teaches us to be exceptionally wary of vague behavioral tools like non-discrimination obligations. They are often, and notoriously, a nightmare to design, to interpret, and to enforce. I do not think anyone should feel enthusiastic about the prospect of agency staff, or a court, trying to figure out whether someone's app isn't prominent enough in the app store, whether an algorithm is producing a search ranking that is "too low," or whether a delay in integration is lasting "too long." Our antitrust agencies have their hands full—more than full, in fact—dealing with mergers and anticompetitive practices, and their time is surely much better spent doing that work. But AICOA doubles down on exactly the kind of thing we normally try to avoid in antitrust enforcement: broad, vague obligations that generate uncertainty, fuel litigation and confusion, and tie up resources.[6] To make it very concrete: I cannot think of any successful FTC or DOJ enforcement action in recent years for violation of a non-discrimination obligation imposed as an antitrust remedy!

Indeed, the current Administration's antitrust agency leadership has repeatedly criticized the effectiveness of complex behavioral remedies to shield consumers from harm, even in specific markets for specific parties with specific remedial concerns in mind (a much easier project than AICOA's wide-angle *ex ante* focus).[7] As Holly Vedova, Director of the Bureau of Competition,

---

[6] The ABA Section of Antitrust Law—whose members will, no doubt, be litigating AICOA issues for many years if the legislation passes—has pointed out a variety of concerns with vague and undefined terms in AICOA. *See* Comments of The American Bar Association Antitrust Law Section Regarding the American Innovation and Choice Online Act (S. 2992) Before the 117th Congress (Apr. 27, 2022), https://www.americanbar.org/content/dam/aba/administrative/antitrust_law/comments/at-comments/2022/comments-aico-act.pdf ("Qualifications like 'preference,' 'limit,' 'materially harm,' and 'materially restrict or impede' inject uncertainty into how the Bill would be administered. These terms are not defined in the Bill and existing antitrust case law cannot be relied upon to supply definitions. . . . If the Bill means to articulate entirely new substantive standards than those applied in current antitrust practice, it should state so explicitly and take steps to further define these concepts to minimize ambiguity. Similar comments apply to concepts like 'products or services . . . that are not part of or intrinsic to the covered platform itself' or 'standards mandating the neutral, fair, and nondiscriminatory treatment of all business users.' . . . The Section recommends that the Bill explicitly define its key terms.").

[7] *See, e.g.*, AAG Jonathan Kanter, *Remarks to the New York State Bar Association Antitrust Section* (Jan. 24, 2022), https://www.justice.gov/opa/speech/assistant-attorney-general-jonathan-kanter-antitrust-division-delivers-remarks-new-york ("Experience shows that it is often impossible to craft behavioral remedies that anticipate the complex incentives that drive corporate decision-making. This is especially true as market realities evolve over time.").

has recently said that in merger cases "[w]e . . . very strongly disfavor behavioral remedies because not only are they very difficult to enforce, but also because *they never seem to work.*"[8]

Third, it may be worth remembering that the rest of the world is closely watching the United States very closely in matters of digital competition policy. Obligations like non-discrimination, forced access to platforms and consumer data, and so on may well inspire other jurisdictions to enact similar, or more intrusive, versions of the same programs. There is no guarantee that such measures will contain robust protections for consumer privacy, intellectual property, or the integrity of commercial data. Congress may have some pause about giving political cover for such legislation elsewhere.

The remainder of my comments on AICOA are in five sections. Section B explains that "self-preferencing" includes a vast array of practices that benefit consumers. Section C explains why banning self-preferencing would harm consumers. Section D explains that the possibility that self-preferencing may be harmful in particular markets does not justify a general ban on the practice—and how a much narrower rule might serve Congress's purposes. Section E explains why AICOA's qualifying provisions—that is, the harm to competition requirement and the affirmative defenses—do not resolve my concerns. Section F explains my concerns with the other provisions in Section 3(a). Section G provides a variety of other comments on the current draft, including comments on AICOA's somewhat arbitrary-seeming scope, and offers technical comments on drafting issues that may be presented by the current bill.

---

[8] Holly Vedova, FTC, *Update from the FTC's Bureau of Competition* (Feb. 3, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/vedova-gcr-law-leaders-global-conference.pdf (emphasis added).

B. "Self-Preferencing" Includes Many Desirable Practices

I take the core of AICOA to be the rule against self-preferencing by covered platforms. This rule is constituted by two prohibitions: Section 3(a)(1) prohibits a covered platform from "preferenc[ing] [its own] products, services, or lines of business . . . over those of another business user on the covered platform in a manner that would materially harm competition"; and Section 3(a)(2) prohibits a covered platform from "limit[ing] the ability of the products, services, or lines of business of another business user to compete on the covered platform relative to the products, services, or lines of business of the covered platform operator in a manner that would materially harm competition." I read these as alternative formulations of a single principle: a covered platform may not treat its own complementary products and services "on" the platform more favorably than those of rivals that are business users.[9] In other words: self-preferencing is presumptively banned. (I will consider the "harm to competition" criterion, and the affirmative defense, below.[10])

The self-preferencing ban would prohibit many product improvements, and other practices that are obviously good for consumers. Whenever an integrated business spots an opportunity to make two or more of its products, services, or divisions work better together, doing so constitutes self-preferencing unless the business also goes to the effort and trouble of doing the same thing, or offering to do the same thing, with a potentially limitless group of external actors.

Platforms may very often, and very reasonably, be unable or unwilling to extend an improvement, feature, integration, or access point to the whole world. There are many technological, commercial, and policy reasons why sharing an improvement with the world—or

[9] This definition may be broader than Congress intends. *See infra* § II.G.4.

[10] *See infra* § II.E.

even giving all applicants some kind of due process—may be unappealing, expensive, risky, or impossible in a particular case. In such cases, the self-preferencing ban will mean that the platform will not be able to implement the improvement. And if that improvement played an important role in some other beneficial activity—for example, entering a new market or line of business—then the platform's ability and incentive to invest in that activity, also, will be squashed.

It may be helpful to consider some specific reasons why a platform might be willing and able to integrate with an internal partner but unable or unwilling to do so with the entire world. Internal trading partners are usually transparent, reliable, predictable, trustworthy, and incentive-aligned in ways that arms-length third parties often are not, and *all conceivable third parties* never are. It may be enormously time-consuming to design, create, and maintain the necessary technological and commercial relations with third parties (*e.g.*, where terms and prices must be agreed, or technological problems solved, or valuable interests protected, to provide the service to a third party). Scarce resources may be involved: file storage space for preinstalling apps or files; page space for displaying links or apps; user time to search through a list of endless options. It may be difficult or impossible to screen third parties—let alone *all* third parties—in sufficient detail to guarantee the quality of their product or service; the security with which they protect user data; their freedom from control by, influence of, or vulnerability to, adversary governments or other hostile and malicious actors; their commitment to maintaining and upgrading a product or service, including regular updates and software patches to maintain security; their honesty, integrity, and freedom from malicious code, spam, or unwelcome practices; and so on.

Coordinating with third parties (above all, with a limitless class of third parties) will often be vastly more hassle—more costly, more time-consuming, more risky, more burdensome—than

coordinating with other parts of a single business. A platform may very reasonably be unwilling to share commercially sensitive information, intellectual property, trade secrets, know-how, business plans, or other investments with third parties who may have the incentive and ability to use that information strategically against the business. And it may simply be more hassle than it is worth to try to create and maintain equal commercial and technological relationships with a potentially limitless cast of third parties, who may be based anywhere in the world.

So there are many, many reasons why dealing with third parties—let alone dealing with *all comers on equal terms*—might be very costly or impossible for a rational platform. But consumers are benefited, not harmed, when businesses take the opportunity to make their products work better together, even when they do not or cannot extend those improvements to all comers.

Real-world examples of beneficial self-preferencing—by covered platforms and other businesses—are plentiful.[11] For example, drawing on both covered platforms and other businesses:

- **Google Maps / Google Search and Bing Maps / Bing.** Showing a Google Maps result as part of a Google Search result for "superb British cuisine near me" is self-preferencing, because Google Maps is treated more favorably than its competitors on Google Search. Microsoft Bing does the same thing with Bing Maps.

[11] There is a complex puzzle raised by AICOA's text concerning the definition of a "business user." Only "business users" benefit from AICOA's protections against self-preferencing. Thus, if self-preferencing takes place in a market where no business users are allowed—such as a fully closed system or part of a system—we might think that there is no AICOA violation. However, the definition of "business user" is broader than it may appear. Section 2(a)(2)(A) generally defines a business user as "a person that uses or is likely to use a covered platform for the advertising, sale, or provision of products or services." Now suppose that Entity X supplies product A and product B in two totally separate markets. And suppose Entity X is a business user of a covered platform through its supply of product B. Product A is not sold on through the covered platform because the covered platform is closed in the relevant market: *no* third party competition is permitted. But AICOA considers Entity X a business user with respect to both A and B. Thus, the operation of a closed system that excludes product A seems to become an AICOA violation. I cannot tell whether this is a drafting error, an intentional choice, or my misreading! Similarly, the definition of "use" is critical in limiting the set of entities that are "business users." Suppose, for example, my landscaping business has a website that can be viewed through the Microsoft Edge browser, or through iOS devices, which is linked from my product page on Facebook, and which gets traffic from Google Search results… am I for that reason a business user of all those platforms? If so, "business user" is an exceptionally broad concept. If not, it is not clear what narrower meaning is intended. *See infra* § II.G.4.

- **Microsoft applications / Microsoft Windows and Sony or Nintendo video games / PlayStation or Switch.** Including some Microsoft applications along with the Microsoft Windows operating system so that a new user enjoys rich functionality out of the box is self-preferencing, because the Microsoft applications are treated more favorably than their competitors on the Microsoft Windows OS. Likewise, including a Sony or Nintendo game along with a new PlayStation 5 or Switch is self-preferencing, because the Sony or Nintendo game is treated more favorably than competing games.
- **Apple apps / Apple iOS.** Pre-installing some Apple apps, like Apple Maps or Mail, on an iPhone so that a new user can use the phone for tasks is self-preferencing, because the Apple apps are treated more favorably than their competitors on the iPhone.
- **Apple hardware / iOS.** Apple's practice of manufacturing all its own hardware and devices for iOS (iPhones, iPads, etc.) is self-preferencing, because Apple's own manufacturing division is treated more favorably than competing manufacturers. So is the introduction of iOS features that work only, or better, with Apple Watch.
- **Prime Video and Amazon Music / Amazon Prime.** Giving Amazon Prime members included access to Prime Video and Amazon Music is self-preferencing, because Prime Video and Amazon Music are treated more favorably than their competitors by the Amazon Prime program.
- **In-house content / Apple+, Amazon, Disney+, and Netflix platforms.** Giving special promotion to in-house content on the Apple+, Amazon, Disney+, and Netflix platforms (*e.g.*, in a carousel at the top of the screen or page) is self-preferencing, because that content is treated more favorably than content from competing creators (indeed, I understand that Disney+ carries only in-house content).

- **Platform / virtual assistant and virtual assistant / in-house apps (Apple Siri, Amazon Alexa, Google Assistant, Microsoft Cortana).** Enabling new ways—or improving existing ways—for a platform to work with an in-house virtual assistant (such as Siri, Alexa, Google Assistant, or Cortana), or for a platform's virtual assistant to work with in-house apps, is self-preferencing, because the in-house virtual assistant or the in-house apps are treated more favorably than third-party rivals.
- **Google Search / Chrome and Bing / Microsoft Edge.** Offering automatic search in the address bar of a browser through a (changeable) default—as Google does with Google Search in Chrome and as Microsoft does with Bing in Microsoft Edge—is self-preferencing, because those search engines are treated more favorably than their competitors on the Chrome or Edge browsers.
- **In-house security tech / any platform.** Integrating a platform's own security (anti-virus, anti-malware) products into a covered platform is self-preferencing, because those products are treated more favorably than their competitors on the platform.

Combinations and improvements like this are clearly good for consumers. Indeed, these are the very kinds of complementarities that courts and agencies routinely identify as a *benefit*, not a harm.[12] When antitrust enforcers exhort digital platforms to "compete on the merits" rather than using anticompetitive agreements, exclusionary practices, or anticompetitive mergers, this is exactly the kind of thing that they normally have in mind.

---

[12] *See, e.g.*, Princo Corp. v. Int'l Trade Comm'n, 616 F.3d 1318, 1335 (Fed. Cir. 2010) (noting that procompetitive effects can include "greater product interoperability"); SD3, LLC v. Black & Decker (U.S.) Inc., 801 F.3d 412, 435 (4th Cir. 2015) (noting that joint ventures may have "decidedly procompetitive effects" including by promoting "greater product interoperability"). *See also, e.g.*, U.S. Dept. of Justice & FTC, *Antitrust Guidelines for the Licensing of Intellectual Property* (2017) § 5.5 (noting that certain licensing practices can be procompetitive when, among other things, they permit "integrating complementary technologies"); Statement of Interest of the United States, Cont'l Automotive Sys. Inc. v. Avanci, LLC, Case No. 3:19-CV-02933 (N.D. Tex. filed Feb. 27, 2020), 5 (listing "interconnectivity and interoperability" as "key benefits" of industry standards).

Nor is self-preferencing unique to digital platforms. Far from it: self-preferencing is utterly ubiquitous in our economy. Most businesses in the economy are vertically integrated to at least some extent: that is, they perform more than one function in a supply chain within the bounds of the firm. And most such businesses treat their internal divisions more favorably than arms-length trading partners in at least some ways. After all, businesses often do not allow their full-time employees to perform work on a spot labor market for their rivals: instead, they usually reserve their upstream labor input for their own use. They often do not commonly allow competitors to advertise on their own facilities, to have equal time on their productive machinery, to claim equal shelf space in their retail outlets, to have equal time using the company's delivery trucks, or to have equal space in their warehouses. Some manufacturers may choose to operate retail facilities (whether digital or brick-and-mortar) that offer *only* their own-brand goods, while others might choose to make limited provision to sell other manufacturers' output as well.

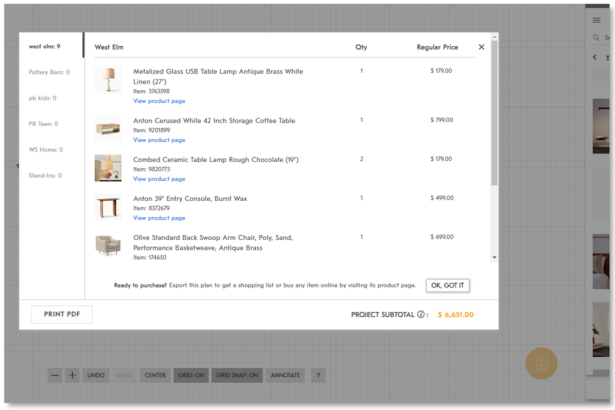
Ultimately: *no business deals on equal terms with the whole world.* Nor would it be possible to do so. Apart from anything else, resources are scarce. There is a limited amount of shelf space in a supermarket, a limited number of pixels on a computer screen, a limited volume of storage space on a device hard drive, and limited time for a business to maintain commercial and technological relations with third parties.

To make this very concrete—and to demonstrate how ubiquitous self-preferencing is and how desirable it can be—let's take an example from Main Street. The furniture retailer West Elm has a room planner on its website that allows consumers to build up a 2D and 3D image of a room, so consumers can figure out what will fit in their homes.[13] The planner has a "Furnish" menu on

[13] https://www.westelm.com/pages/ideas-and-advice/room-planner/.

the right hand side that shows images of furniture sold by West Elm (and other brands under common ownership like Pottery Barn). Consumers can drag and drop these furniture items onto the room planner, whereupon—because West Elm knows the dimensions, available colors, and shapes of all its own furniture—they turn into 2D and 3D versions that can be moved and recolored.

After the consumer has finished furnishing the room, clicking "View Plan Items" brings up a digital checkout with an opportunity to buy the items.



This is, of course, self-preferencing: the in-house furniture store is preferred over all other rival furniture stores. It is clearly beneficial to consumers. And of course West Elm would not do this kind of thing if it had to make this platform available to all other furniture suppliers on equal terms: the technological and commercial burdens would be absurd. Nor would it make commercial sense to do so: it makes sense to offer consumers the room planner service for free *because* it is a desirable form of distribution for West Elm's furniture business.

One sometimes hears broad claims that digital markets are different, and that practices that might be untroubling for, say, a supermarket monopolist, may be harmful for a tech monopolist. Certainly, the digital nature of some products and services—as well as platform dynamics, network effects, data, and the other peculiarities of some digital markets—can be important in some cases in some ways. But there is no general reason to think that online markets *in general* are more monopolized than brick-and-mortar ones.[14] For example, plenty of supermarkets, grocery stores,

[14] For a good recent discussion, *see* Herbert Hovenkamp, *Gatekeeper Competition Policy* (Feb. 2023), 6 et seq., https://ssrn.com/abstract=4347768.

and other suppliers in rural communities enjoy much larger shares of their respective markets than Amazon's 38% of e-commerce[15] (with e-commerce itself less than 15% of all retail sales[16])—and the barriers to buying from an alternative supermarket may be very much higher.[17]

Most importantly: *a product improvement is still a consumer benefit even when it is introduced by a digital monopolist!* The integration of Google Maps content into a Google Search result is still a consumer benefit even though Google may have monopoly power in search. The inclusion of Microsoft applications with the Windows operating system is still a consumer benefit even though Microsoft may have monopoly power in PC operating systems. And so on. Indeed, some digital markets may offer *more* opportunities for complementarities and interoperabilities—given the suitability of software for updates and integration—than some brick-and-mortar markets do. And the broader the user base of the improved product, the greater the resulting social benefit.

I have focused so far on product improvements that involve integration, but a self-preferencing ban would also deter other beneficial practices. For example, self-preferencing—in the form of some kind of special promotion or distribution—often plays a role in incentivizing and supporting a platform's fresh entry into a new market. Indeed, the possibility of such promotion (and the opportunity to drive value and demand for the integrated business) may be central to the decision to invest in the first place. For example, Amazon and Apple+ (and Disney+ and Netflix, for that matter) all engage in special promotion of their own in-house content on their own

---

[15] Statista, *Market share of leading retail e-commerce companies in the United States as of June 2022* (June 2022), https://www.statista.com/statistics/274255/market-share-of-the-leading-retailers-in-us-e-commerce/

[16] U.S. Census Bureau News, *Quarterly Retail E-Commerce Sales 4th Quarter 2022*, https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

[17] It is worth remembering that in some communities, supermarkets exercise true monopoly power. In a rural community with just one supermarket, residents—including residents who may not own cars—may find it much more burdensome to travel a long distance to an alternative food store than they do to type a different URL into their browser.

platforms. The incentives of Amazon, Apple, and Netflix to invest in new content creation were clearly augmented by the opportunity to use their respective platforms to promote, and drive demand for, that content.[18]

Consumers seem to have benefited as a result. Apple has invested in shows like *The Morning Show*, *Severance*, *For All Mankind*, and *Ted Lasso*. Netflix has invested in shows like *The Crown*, *Stranger Things*, *The Witcher*, and *Formula 1: Drive to Survive*. Amazon has invested in shows like *The Lord of the Rings: The Rings of Power*, *The Legend of Vox Machina*, and seasons 4-6 of *The Expanse*. And so on. (Your own preferences may vary!) If these platform owners had been prohibited from promoting their own content on their respective platforms, the costs and risks of these investments would have been greater, and their incentives to invest reduced.

In addition: self-preferencing also includes certain kinds of low pricing by integrated businesses. Integrated businesses routinely find it rational to price an internal transfer between divisions at lower than the price it charges to unintegrated purchasers. (I am setting aside the vast practical difficulties associated with cost accounting within the firm, to isolate the theoretical point.) Some of this effect can arise from differences in transaction costs: the fact that it is often cheaper—less costly, less risky, less burdensome—to deal with another part of the corporate enterprise than to deal at arms' length. A second effect can arise from the fact that the supplier of, say, an input, has an extra incentive to lower its price to an internal trading partner because it will share in that trading partner's own profits. This is sometimes called the elimination of double

[18] Disney seems differently situated, as Disney was a content creator first. In Disney's case, though, the value of self-preferencing probably goes the other way. The value of Disney's content, including newly acquired brands like Marvel and Star Wars, certainly helped to drive demand for the Disney+ platform. No doubt the incentive to build out the platform was influenced by the opportunities for special promotion of this content. But the underlying point—that the combination of complementary assets is a powerful engine for consumer benefit—holds here too.

marginalization: the point is that each component of the firm is not optimizing its own profit in a vacuum because the other component benefits from a price reduction. The result is that it prices lower. This effect can certainly give the integrated firm an advantage over rivals that buy inputs from the merged firm, but consumers benefit from the lower price, compared to a world in which the business had not entered at each level. (Of course, if the business has achieved integration through a vertical *merger* rather than building out its own capacity, the effects are more ambiguous: in that case, there may also be a loss of competition to weigh against the benefits. But that is not this case! We are just talking about new organic entry.)

To sum up: a ban on self-preferencing would deter a wide array of beneficial practices.

C. Banning Self-Preferencing Would Inflict Consumer Harms

A ban on self-preferencing would threaten harm to consumers in multiple ways. In particular, it would deter platforms from: (1) implementing product improvements and other beneficial practices; (2) protecting users in close cases; (3) using certain ad-supported business models; (4) operating closed ecosystems. And it would also: (5) deter interplatform competition *against* covered platforms.

1. A Ban Would Deter Product Improvements

First, and most obviously, a ban on self-preferencing would deter platforms from engaging in the beneficial practices described in the previous section, including various forms of product improvements, feature innovations, new market entry, and lower pricing.

Suppose, for example, that a product design team at a covered platform has spotted an opportunity for a product improvement that involves linking two of the platform owner's products

or services together in some way. The business is deciding how to allocate time and resources, including whether and to what extent it will invest in the proposed product improvement. The product design team will understand that an obligation to extend equal treatment to rivals will often be costly. Recall that "equal treatment" here could take any of a wide variety of forms, such as: (1) pre-installing rivals' software or applications on devices; (2) including rivals' products or services in bundles that are sold or made available to users; (3) including links or buttons to rivals' products on a webpage or in a system menu; (4) making rivals' apps or products available on a store; (5) linking or integrating rivals' hardware or software to or with a platform; (6) creating options for rivals' products or services to be set as a default for some function or other on the platform; (7) giving equally prominent placement or ranking to rivals' products, icons, apps, or websites in or on screens, menus, results, marketing communications, etc; (8) establishing and maintaining a flow of data or information, including personal, financial, or other consumer data; (9) providing access to sensitive information, technology, business plans, or user data; and so on.

Regardless of the nature of an improvement, providing it for third parties may require time, money, energy, technical challenges, exposure to brand risk, and personnel—perhaps on an ongoing basis. It may require commercial negotiations, and/or policy formulation, about the terms of the relationship and about collateral obligations needed to protect user data, system integrity, or the quality of the product. It may require screening or auditing the third parties on an ongoing basis for an array of policy concerns like data privacy, spam, bugs, hostile or malicious code, or technical integrity and compatibility. It may require ongoing communications with the third party (or with others like consumers) regarding complaints or technical questions. And even if the platform does not ultimately grant access, some kind of due process may have to be afforded third parties to comply with the equal-treatment of obligation: including third parties with low-quality, high-risk,

or objectionable products. (Of course, sometimes equal treatment will be easy: the point is that it may often not be.) The product design team considering the proposed improvement will foresee these costs and hassles, and they will make investment in the proposed improvement less appealing.

The point should be clear. Instead of running an innovative business, our product team could find itself planning for life as a *de facto* utility, serving all comers on equal terms. But, whereas traditional utilities like water companies generally supply a single undifferentiated product to a finite local community, the product team in our example is dealing with a potentially limitless collection of unknown applicants presenting a rich and unknown variety of challenges.

To make this very concrete, take the example of the integration of Google Maps with Google Search. What would it mean to make that integration available on equal terms to all other third-party mapping products? The universe of such mapping products is potentially limitless, including: low-quality products that work badly, crash, are not often updated or corrected,[19] or convey inaccurate information; products and product owners that would compromise data security, user privacy, or carry malicious code or surveillance tools; products that are "spammy" and drown the user with low-quality advertisements, pop-ups, and junk content; products owned or controlled directly or indirectly by threats to national security and to user welfare; and products that are burdensome or difficult to integrate.

[19] Regular updates are a crucial means of protecting users against threats. *See, e.g.*, Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 14 ("[T]he number of security vulnerabilities discovered each year is on the rise. Many of these vulnerabilities are being found through rigorous testing by quality assurance and penetration testers. However, a significant number are also being discovered and exploited by rogue actors — with many of them identified only after a breach has been observed and proof-of-concept code has been shared openly. Keeping internet-connected devices and applications up to date is the best way to defend against the growing number of vulnerabilities — but many are not or cannot be updated — As a result, they remain vulnerable to botnets, often serving as gateways for more sophisticated attackers to gain a foothold into a network.").

And to make it more concrete still: is Google required to accord equal treatment in Google Search results to "Russian Hacker Maps"—a hypothetical mapping product produced at the direction of Vladimir Putin's government and operated by a nominally private entity in the interests of that government—integrating it into Google Search in just the same way as Google Maps? Is Apple required to preinstall it on the iPhone if it wants to preinstall Apple Maps?

Surely not, of course. *But now suppose that Russian Hacker Maps is sophisticated enough to call itself "USA Trusty Maps," and to disguise its ownership and control through a Delaware corporation or two.* Are Google and Apple really required or expected to accord equal treatment to "USA Trusty Maps" until they have investigated sufficiently to have discovered the link to the Russian state apparatus? How much investigation can we possibly expect them to perform?

The answer is that, of course, no detailed investigation is possible. There are currently something like 3.5 million apps on the Google Play Store and 1.6 million apps on the Apple App Store.[20] The vast hassle and expense of grappling with problems like this one will not encourage platforms to undertake detailed investigations: instead, it will simply deter them from integrating Google Maps, or preinstalling Apple Maps, in the first place. Consumers lose.

It is also worth pointing out that equal treatment obligations may also have some "second order" effects resulting from *actual compliance* with AICOA by a platform. This includes congestion, confusion, and quality degradation. It is not obvious that consumers would really be benefited overall if Google replaced the single high-quality Google Maps mapping function with, say, a lengthy "choice menu" inviting consumers to choose from among an endless list of mapping

[20] Statista, Number of apps available in leading app stores as of 3rd quarter 2022 (Oct. 2022), https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

providers of variable quality. (After all, who could be excluded?) Less sophisticated users in particular may face a series of complex choices among similar-sounding options that they are ill-equipped to navigate, ending up with a worse or unsafe product as a result.

We would have no time at all for an idea like this in almost any other context. Suppose that anyone who cared to set themselves up as a supplier of food or consumer products had an affirmative presumptive right to be carried on Walmart's shelves, subject to narrow defenses for which Walmart bore the burden of proof, on pain of injunctions, penalties, and compensation forfeiture. We would all be horrified—even if we thought Walmart was going to be a monopolist until the end of time. We would fear that the shopping experience would be fatally compromised by a deluge of low-quality products, and the costs of sorting through them to find the few that Walmart would have chosen to carry. And we would *deeply* fear for the well-being and safety of consumers. But this is precisely the result that AICOA threatens.

2. A Ban Would Deter Platforms from Protecting Consumers

Just as a self-preferencing ban would deter beneficial product improvements, so too it would also deter, on some important margins, *desirable* denials of service.

Recall, as we noted above, that the universe of third parties seeking equal treatment is potentially limitless. Some of those parties and their products will be technologically unreliable or unstable and prone to crashing; some will provide false or inaccurate information; some will just be badly designed, poorly maintained, or not updated; some will be saturated with spam; some will be vehicles for objectionable content, like sexually explicit conduct or the promotion of terrorism and violence (and some will disclose this fact, while others will conceal it); some will

contain computer viruses or other malicious code; some will be operated by criminals in search of personal information; some will be compromised by national-security threats; and so on.

We can call this entire group "bad actors." They need not be subjectively culpable or malicious—although many certainly will be—just harmful overall to consumers.

Today, platforms can deny access—whether through individual determinations or through the application of general policies—when they have concerns that they might be dealing with bad actors, regardless of whether the platform could (or would be willing to) produce a robust evidentiary showing to support its decision.

But a self-preferencing ban would profoundly change this situation. Bad actors would presumptively enjoy a right to equal treatment with the platform's own products and services. Certainly, the current draft contains some affirmative defenses, but as explained below these are very limited (including because they are subject to a demanding less-discriminatory-alternative test, do not cover many important policy grounds, are fact-intensive, and place hefty burdens on the denying platform). A platform will not be particularly enthusiastic about going ten rounds with the FTC over whether some aspect of its security policies, or quality standards, are unduly high. And, as noted below, the platform will know that an agency investigation may involve the application of interim injunctive relief on a specially-lowered standard,[21] as well as the risk of litigation and penalties. Complaints will mean the threat of serious disruption, delay, and cost.

This problem will be seriously exacerbated by the prospect of compensation forfeiture pursuant to Section 3(c)(6)(D). I cannot imagine a more effective way to undermine platform

[21] *See infra* § II.G.7.

security than threatening to take compensation away from individual decision-making executives if they deny access one time too often.

Certainly, it helps that AICOA enforcement is not in the hands of private parties and competitors, but rather with federal and state enforcers.[22] But this does not resolve the concerns. First, and most importantly, the *threat and risk* of complaints, investigations, interim relief, and litigation will have plenty of deterrent effects before an enforcer gets anywhere near the issue. Negotiating parties will make many, many demands of covered platforms, backed by threats of complaints (including to State AG offices, which may have different perspectives from the federal enforcers). Only one State AG is needed to open an investigation! Second, every enforcer investigates plenty of cases that turn out not to be suitable for prosecution. Even an investigation may well mean plenty of trouble, burden, cost, and delay—especially given the specially lowered threshold for interim injunctive relief in AICOA. Third, each of the 50+ government enforcers may turn out to have very different views about the best reading of AICOA or about the most suitable cases for investigation. And, fourth, even government enforcers might themselves not in every conceivable case take the most pro-consumer views of AICOA's meaning and terms—even with the best of intentions.

The point is that on some very important margins, the creation of a general background duty to deal will incentivize the platform to cave in in close or borderline cases, and to grant access that it would otherwise have denied. This will include cases where the platform has concerns but does not think it would be able to prove them on the balance of probabilities, as well as cases in which the platform simply does not want to go through an extensive (and expensive) defense of

[22] *See* letter dated July 7, 2022, from Fiona Scott Morton and Steven Salop to Senators Klobuchar and Grassley, https://som.yale.edu/sites/default/files/2022-07/AICOA-Final-revised.pdf.

the bounds of, and evidentiary support for, its various rules and decision. On the margin, more bad actors will gain access to the platform, to data, and to consumers.

Bad actors of various kinds are plentiful on digital platforms and plentiful in the world.[23] It is not at all clear why we would want to make it harder for platform owners to keep their platforms clean, and ensure the quality and safety of their offerings, at this time.[24] The ongoing explosion of online-enabled devices (the "Internet of Things") means that digital vulnerabilities are an increasing threat not just to consumers' devices and data, but also to their homes.[25] As the UK's National Cyber Security Center has warned, for example: "voice assistants represent an

---

[23] *See, e.g.*, Crowdstrike, 2023 Threat Report, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf, 2 ("[A]dversaries have become more sophisticated, relentless and damaging in their attacks. As a result, a number of disruptive trends emerged in 2022 that threaten productivity and global stability. . . . nation-state attacks coincided with organizations struggling to manage an explosive landscape of vulnerabilities that amplified systemic risk."); Sophos 2023 Threat Report, https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf, 3 ("[A]dversaries have not stopped trying to discover and exploit vulnerabilities, and in fact seem to have stepped up efforts designed to subvert the security of every vendor's firewalls, switches, and network access points."), 6 ("Access brokers, ransomware, information-stealing malware, malware delivery, and other elements of cybercrime operations have lowered barriers to entry for would-be cybercriminals.").

[24] I note that an array of former military and intelligence leaders have expressed concerns regarding AICOA's implications for national security. *See, e.g.*, Glenn S. Gerstell, *Before we regulate Big Tech, let's make sure we don't hurt national security*, THE HILL (May 19, 2022) ("Mandating that a third party has the right to connect and operate seamlessly with a platform's own systems could, for example, mean that the platform couldn't scan for or block malicious code; the platform does indeed have to "discriminate" against bad software. Yet, depending on the interpretation of the bills' provisions, that might be unintentionally outlawed. Obviously, curtailing a platform's ability to prevent a computer virus from infecting that platform or its users, or allowing disinformation to be posted and disseminated, can't be good for our national security."); Robert C. O'Brien & Jeh Johnson, *The Big Tech Battlefield*, NEWSWEEK (May 19, 2022) ("Legislation pending in both the House and Senate would require non-discriminatory access to U.S. digital platforms for all 'business users,' including foreign ones. This could potentially require U.S. platforms to broadcast the false propaganda of autocratic regimes—a step backward in U.S. efforts to combat harmful foreign disinformation and even attempts by our adversaries to influence our own elections. Other parts of [AICOA] would constrain U.S. companies from removing malicious actors and integrating cybersecurity tools to their platforms, possibly leaving U.S. tech infrastructure vulnerable to America's foreign adversaries. These national security risks have been acknowledged by the legislation's sponsors. Nevertheless, they have not been addressed as part of any meaningful review of the legislation for their implications to U.S. national security."); Letter to Hon. Nancy P. Pelosi & Hon. Kevin O. McCarthy from Robert Cardillo, John D. Negroponte, Dan Coats, Leon Panetta, et al., https://www.documentcloud.org/documents/21062393-national-security-letter-on-antitrust ("The recent U.S. Innovation and Competition Act (USICA) has the potential to put us on strong footing to compete with China. . . . .Recent congressional antitrust proposals that target specific American technology firms would degrade critical R&D priorities, allow foreign competitors to displace leaders in the U.S. tech sector both at home and abroad, and potentially put sensitive U.S. data and IP in the hands of Beijing. . . . [W]e believe more deliberate analysis is needed to examine the detrimental impact these bills could" have on our strategic competition with China. Congress should not proceed with current legislative proposals before understanding the full range of potential consequences.").

[25] *See, e.g.*, Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 7 ("Cybercriminals have shifted their focus to IoT and mobile devices"), 14 ("From 2019 to 2020, there was a 100% growth in IoT device infection rates.").

attractive target for attackers, who could use them to steal personal data and listen in on victims' conversations."[26]

Moreover, serious threats are commonly disguised as benign apps, and sometimes slip into even official app stores. Nokia's 2021 Threat Intelligence Report explains some of the sophisticated ways in which major threats disguise themselves in an effort to reach users:

> The number of Trojans [a form of hostile tool used by criminals and malicious actors] targeting banking information through Android mobile devices has skyrocketed, putting millions of users around the world at financial risk. Malware app developers are getting better at bypassing the security measures intended to keep harmful apps out of official app stores . . Banking Trojans can arrive on smartphones in a variety of ways, often disguised as common and useful apps.
>
> [. . .]
>
> FluBot is typically disguised as a package tracking app from a major courier company. The user receives an SMS message indicating that a parcel is being delivered and is offered a download link to a bogus tracking app.
>
> [. . .]
>
> TeaBot comes disguised as a video app (or other useful app) to trick the user into installing it. When run, the app acts as a remote access Trojan, allowing its distributor to exercise considerable control over the infected device.
>
> BlackRock was first discovered in 2020 and is typically disguised as an Android or Google update, distributed through a third-party app store. Like other banking Trojans, it uses login screen overlays and SMS message capture to acquire banking credentials, but it also tries to gather additional personal information from the phone and installed apps, including dating, shopping, lifestyle and productivity apps.
>
> Cerberus has been around since 2019 and is "leased" to malicious actors wishing to distribute it to collect banking credentials in their region. It operates similarly to other Android banking Trojans, but more modern versions also leverage TeamViewer to allow the author to gain remote access to the device.
>
> Mandrake is a highly sophisticated spyware package focused on gaining access to financial information and credentials. This Android threat has been around for five years and has seen bug fixes and feature enhancements added to it over that time. Typically, Mandrake gets installed via a benign-looking dropper app in Google

[26] UK National Cyber Security Center, Threat Report on Application Stores (2022), https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf, 11.

> Play or a third-party app store. Once installed, the dropper app installs Mandrake disguised as a system application, such as a firmware update.
>
> Banker.GXB may be disguised as a variety of useful tools, including power managers, storage cleaners, performance boosters and horoscope utilities, originally found in the Google Play store in 2018. Like other banking Trojans, Banker.GXB impersonates legitimate banking applications and steals SMS messages. Unlike most banking apps, which never provide their promised functionality, Banker.GXB apps at least provide the appearance of performing their intended function to avoid suspicion.[27]

As Congressman Eric Swalwell has pointed out, and as I describe further below,[28] AICOA's "modest defenses" would "require an unwieldy amount of evidence for each and every action the platform makes to protect our national security. This is especially concerning where decisions must be immediately made to limit widespread damages . . . [and the result would] blunt platforms that are working closely with intelligence communities to strengthen our homeland."[29]

To be clear, I do not mean to suggest that *only* bad actors will benefit. The self-preferencing ban will doubtless allow some more non-bad actors to gain equal access too, and that could be good. But I doubt the social harm from letting, say, Russian Hacker Maps (whether or not re-branded "USA Trusty Maps") onto the Apple App Store, or Russian Hacker Word Processor onto Windows PCs, or Russian Hacker Camera App onto the iPhone, would be offset by the social benefits of admitting three or ten or fifty other small independent software developers as well.

3. A Ban Would Challenge Some Free-to-Use, Ad-Supported Services

Third, a ban on self-preferencing may challenge certain free-to-use, ad-supported business models that allow consumers to enjoy valuable services without paying a fee. In particular, a ban

---

[27] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 17–18.

[28] *See infra* § II.E.1. (affirmative defense), § II.G.10 (exceptions).

[29] Eric Swalwell, *The federal government must address national security concerns in antitrust reforms* (May 10, 2022), https://cyberscoop.com/the-federal-government-must-address-national-security-concerns-in-antitrust-reforms/.

may encourage a shift toward fee-paying, subscription-based models, and that shift may leave users with less money in their pocket.

Today, many digital services are provided by platforms to users for free (or at a low cost), supported by advertising. That system can work successfully *as long as the business can ensure that consumers of the services are also exposed to the advertising mechanism*. But if the business may not promote its own advertising to service users, then it may be unable to expose consumers to the advertising. It may then no longer make sense to provide the service for free. The result may be that the business is pushed toward a fee-paying, subscription-based model.

The point is that reserving exclusive access for a platform's own advertising business seems to constitute the preferencing of the platform owner's own advertising business, or of a product or service that carries or supports it, on the platform. For example, Google sells advertising beside Google Search results and in Gmail inboxes; Meta sells advertising space in the Facebook and Instagram content feeds; Twitter sells advertising space in the Twitter news feed through "promoted tweets"; Amazon sells advertising space in the Amazon product search results through sponsored ads; and so on. Doing so appears to constitute self-preferencing of these platforms' own advertising businesses over those of actual and potential rival advertising businesses on the platform—at least as long as those advertising businesses constitute "business users."[30] And Google's willingness to make the Android operating system available for free is presumably in at least some relationship with the fact that Google's own apps—which support its advertising business—are typically preinstalled on Android devices. Banning that would strike right at the heart of the free-to-use business model.

[30] *See infra* § II.G.4.

My own view is that American families benefit *hugely* from the widespread availability of free digital services.[31] Free-to-use internet search, mapping and navigation, email, video sharing, personal social networking services, microblogging, and so on: at a minimum, it is not unreasonable to think that that is a more than fair trade for getting advertisements for products and services that are of real interest to us, instead of those that are not! Of course, there is plenty of room to take a different view: some would no doubt prefer to pay subscriptions and be free from digital ads. Moreover, without a doubt, digital advertising raises real and serious concerns relating to data privacy and data security: these concerns deserve careful attention from legislators.

But the core point for competition policy is that consumers are probably doing better overall because businesses can choose to offer, and consumers can choose to accept, a free service that comes with an advertising channel bundled in. Congress may want to carefully weigh the consequences of a self-preferencing ban that would challenge that business model.

4. A Ban Would Threaten Closed Ecosystems

Many platform operators choose to "close" some complementary markets on their platforms: that is, to reserve some complementary activity on a platform *wholly* for the platform owner, without third-party competition at all. For example: I understand that Apple does not generally allow third-party smartphones or tablets into its iOS ecosystem, nor third-party app stores; Amazon does not allow third-party music or content stores on the Amazon Prime platform in competition with Amazon Music or Prime Video; and so on. And, looking beyond the covered

[31] *See generally, e.g.*, Erik Brynjolfsson, Avinash Collis & Felix Eggers, *Using Massive Online Choice Experiments to Measure Changes in Well-Being*, 116 Proc. Nat'l Academy of Sci. 7250 (2019); Erik Brynjolfsson, Avinash Collis, W. Erwin Diewert, Felix Eggers & Kevin J. Fox, *GDP-B: Accounting For The Value Of New And Free Goods In The Digital Economy*, NBER Working Paper 25695 (Mar. 2019); The Economist, *How much would you pay to keep using Google?* (Apr. 25, 2018), https://www.economist.com/graphic-detail/2018/04/25/how-much-would-you-pay-to-keep-using-google.

platforms, I understand that Disney and Paramount generally do not carry third-party content, or much third-party content, on the Disney+ and Paramount+ platforms. I understand that the major console manufacturers—Nintendo, Sony, and Microsoft—do not allow third-party online game stores, nor do they allow third-party consoles in their own ecosystems.[32] And so on.

The current draft of AICOA appears to prohibit fully or partly closing a digital platform, because closure is simply an extreme example of self-preferencing, as long as at least one excluded business was a business user of the covered platform.[33] But a ban on closed systems seems undesirable.

There are many good reasons why a business might choose to operate on a closed model. Among other things, a closed system allows the business owner to ensure and vouch for the quality and consistency of the user experience from end-to-end, without running the risk that consumers will have bad experiences because of third-party actions, or the risk that the integrity and quality of the system will compromised by hostile, incompatible, or just bad-quality code. Closed systems, in which the platform owner either allows no entry or directly supervises all third-party entry, have long been widely understood to be more secure than open systems: this has long been a key advantage of the iOS smartphone ecosystem, for example.[34] For example, a 2021 cybersecurity

---

[32] There is some cross-platform interoperability at the individual game level. *See, e.g.*, Wes Fenlon, *Sony charges for crossplay support to protect PSN revenue, documents show*, PC GAMER (May 4, 2021). But third party OEMs cannot build consoles to run, say, Nintendo Switch games in the way that they can build devices to run the Android mobile OS, or Windows-compatible PCs.

[33] *See infra* § II.G.4.

[34] *See, e.g.*, *Can iPhones get viruses? Here's what you need to know*, MARKETS INSIDER (Mar. 4, 2019) (describing the "walled garden" of iOS and noting: "For the vast majority of everyday users, there's virtually no risk of viruses on the iPhone."); Steve Sande, *Why Apple's "walled garden" is a good idea*, ENGADGET (July 29, 2010) ("Many developers and users of Apple's iOS devices bemoan the 'walled garden' of the App Store approval process, but it appears that the company's measures have prevented mass data theft from iPhones, and iPads."). Of course, no system is *free* from threats: and bad actors target iOS as they do any other platform. The point is that more openness means more risk, and that iOS is generally safer for that reason.

threat report published by Nokia notes that the closed model of Apple's iOS has been instrumental to its security, by comparison with Google's more open Android ecosystem:

> While Google has taken an open approach to app development and distribution, Apple has always maintained a proprietary approach, allowing downloads only through the official App Store. *As a result, Apple products have generally been considered the most secure mobile computing platform.*[35]

It goes on to point out that "Android devices make up 50.31% of all infected devices," with iOS far behind.[36] And, as you might expect, Apple trumpets this disparity in making its own case for the closed model: "Over the past four years, Android devices were found to have 15 to 47 times more malware infections than iPhone."[37] It is not clear why Congress would want to prohibit businesses from offering—and consumers from choosing—this valuable business model.

Of course: if closed systems are *permitted* under AICOA (perhaps because the definition of "business user" was narrowed), then a self-preferencing ban would encourage systems that were previously open, but which relied on some distinctive promotion for the platform owner's own products, to consider closing entirely as an alternative. I am not sure that either Congress or consumers would welcome that result.

5. A Ban Would Suppress Interplatform Competition

AICOA would have a particularly perverse impact on competition with the digital platforms themselves: namely, it would *discourage* and suppress inter-platform competition.

---

[35] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 18.

[36] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 8 (emphasis added).

[37] Apple, *Building a Trusted Ecosystem for Millions of Apps: A threat analysis of sideloading* (Oct. 2021), https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf, 2.

The economic point is a simple one. By guaranteeing trading partners specially favored treatment on covered platforms, AICOA would make those platforms a particularly cosy place for businesses that would otherwise have stronger incentives to create, sponsor, or deal with *rival* platforms. After all, why go to the trouble of developing or supporting a rival platform when the terms of dealing with an incumbent like Google or Amazon have been made specially favorable by AICOA? And even if a promising rival *does* emerge, potential trading partners will have less incentive to switch over and take a chance on it, because that rival—unlike the incumbent—will not be subject to AICOA's obligations to provide equal treatment, preinstallation, favorable search rankings, interoperability, and so on. Thus AICOA would turn potential competitors, and sponsors of competitors, into stakeholders in the status quo.

I think it would be a profound mistake to sacrifice competition *with* today's generation of digital platforms, in the hope that society can make do with competition *on* those platforms. And the mistake would be worse still if we weaken even on-platform competition too by restraining the platforms themselves from competing vigorously in such markets.

I think our best hope for dynamic digital markets lies in a world in which Google, Meta, Apple, Amazon, and Microsoft must continue to compete just as vigorously as they can against existing and new rivals—including each other—constrained by robust antitrust enforcement and constant changes in technology and demand. Entrenching their dominance by turning would-be rivals into cosy collaborators, while limiting platforms' own vigor, seems to have everything backwards.

D. The Risk of Harmful Self-Preferencing Does Not Justify a Total Ban

1. Harmful Self-Preferencing is Possible But Elusive

Of course, one can imagine forms of self-preferencing that do not involve genuine or arguable product improvements and which may harm consumers. (I will set aside behavior that would violate existing antitrust law.[38])

Commentators have often focused on search ranking manipulation. Suppose, for example, that an e-commerce website degrades the search rankings for all third-party products, bumping its own products to the top, above rivals' higher-quality products. Or suppose that a search engine degraded the search rankings for all vertical search competitors, bumping its own to the top above higher-quality offerings from rivals.

This is a dangerous game for a platform to play. Manipulation of this kind would inflict a double harm on a platform's market position: (1) it would make the platform less valuable to third-party business users (like merchants or publishers), by reducing their sales or traffic, and (2) it would make the platform less valuable to consumers, by serving up lower-quality results. And, in many platform cases, each of these first-order impacts would in turn have a second-order impact on the other side. That is: as frustrated users turned away from an e-commerce site that was manipulating its results, value for merchants would decline yet more; as merchants dropped off the platform, users would find less value there as well.

[38] This could plausibly include unlawful uses of exclusivity and tying. The application of tying law to self-preferencing is tricky and case-specific: certainly, the inclusion of a free product or service in a package can be analyzed as tying, but on almost any plausible view, merely adding a new function to a product without more would almost certainly not violate antitrust law on a tying theory or otherwise. *See* United States v. Microsoft Corp., 253 F.3d 34, 90–91 (D.C. Cir. 2001). EU competition enforcers have at times taken a different view. Case T-201/04, Microsoft Corp. v. Commission (imposing liability on Microsoft for supplying Windows Media Player along with Windows).

Importantly, trading partners do not have to know that the platform is manipulating anything for self-preferencing to drive them into the arms of rivals. They just have to know their own experience: say, their satisfaction with search results, or their sales or traffic.

Thus, we would usually expect that the platform would earn more profit by *avoiding* manipulation and instead by trying to maximize output and activity on the platform, which it can then monetize by charging users on one or both sides. This way it maximizes its own profits.

But we can imagine at least two theories of anticompetitive harm from manipulation and equivalent behaviors. On one theory—let's call it "Platform Moating"—the platform is aiming to protect the primary platform monopoly by cutting off actual and potential rivals from platform services so that they find it harder to develop into competitors of the main platform. On the other theory—let's call it "Platform Leveraging"—the platform is aiming to acquire a second monopoly in the complementary market.

Self-preferencing that is harmful in the first way—that is, Platform Moating—is likely to be confined to some rare and special cases. For one thing, the platform is lowering quality to *all* customers on both sides: it is annoying consumers who are being steered away from what they really want, as well as trading partners who are getting fewer sales on the platform. By self-preferencing, the platform is actively driving both sets of annoyed customers to seek and support, or become, platform rivals.

By hypothesis, of course, the platform is doing this in order to hit the trading partners who are competitive threats of the platform, but these are likely to be few in number compared to the number of impacted businesses (because most platform customers are not even possibly platform competitors). Moreover, these may be the very competitors who are *most* likely to be able to

manage without the platform, or to give a significant boost to rivals. Self-preferencing gives them a hefty nudge to make the jump into platform competition *and* it incentivizes other users to sign up as their customers. So a platform would have to be really sure it was worth the trade on some unusual facts to think of this as a particularly appealing means of protecting platform monopoly. Nevertheless, "unusual" doesn't mean "never," and it is possible to imagine cases of this kind.

Cases in this first category also seem likely to overlap in practice with cases where the platform prefers its own products or services but has a legitimate basis for doing so: for example, because the platform has more information about its own offering, more control over it, or better ability to guarantee quality. Moreover, with respect to search rankings in particular, it is important to appreciate that there is no "objectively correct ranking principle" that explains how to weigh the benefits of in-house knowledge and control against other things that might plausibly matter to consumers. For example, an e-commerce platform like Amazon or Walmart.com is better able to make sure the quality and timeliness of products that it controls, than of products that are supplied by third parties. Likewise, Apple has greater control over the quality, security, and update frequency of its own apps than of those of app stores. One might think these perfectly sensible reasons to elevate this in-house content in search results or other placement rankings. (Of course, others can disagree! The point is that there is no "objective" position here.)

The second theory—Platform Leveraging—applies to markets where the platform believes that it can plausibly obtain market or monopoly power in the complementary market by degrading platform service and that it will do better by doing so. If the secondary market is materially broader—in that there are many sources of supply beyond the reach of the platform—then the goal of market power in the secondary market is probably unattainable and this strategy will just reduce

the platform's profit (by substituting the platform's less efficient output for the third party's superior output). It is most likely to be a concern in markets where scale economies are vital and the platform itself is a very important input into (or distributor of) most or all activity in the market.

The difficulty with cases of this second kind is *not* that they will almost never exist: it is, rather, that they often be very difficult to distinguish from product-improvement cases and it is very hard to craft a rule that doesn't punish a ton of beneficial conduct. The platform is giving higher-quality supply to its own unit and lower-quality supply to third parties. How should we tell whether this involves a good, desirable improvement of the platform's own products or services or a bad, wasteful degradation of rivals' products or services in the hope of a second monopoly?

Take, for example, a games console manufacturer that also makes games. Suppose it develops a technology for making its own-developed games ultra-realistic on its own console, and does not share that technology with third-party game developers. (Perhaps the technology involves projecting the user's face onto an in-game character, and the manufacturer does not want to get into the business of screening and supervising third party developers' data security, or implicitly warranting that security to users.) How can we tell if this is good or bad self-preferencing? Should it matter if the manufacturer had *first* tried to make the feature available to other developers, only to later find that it was too expensive, risky, burdensome, or unpopular with users, to do so? Should we make legality of identical conduct turn on subjective intention: that is, on whether the key executives were literally thinking "we will make our games better" or "we will make rivals' games worse"? What if executives had different subjective purposes in signing off on the course of action? I am not sure there is any good way to do this sensibly: at a minimum, it subjects product improvements to all the burdens of investigation and litigation described above.

Take a real example. With the release of iOS 15, Apple eliminated some support for certain Siri tools that had been previously made available to third-party developers, through an API deprecation.[39] On the face of it, this is equally consistent with a recognition by Apple that the company's product-improvement plans were not compatible with support for these tools (*i.e.*, a good product improvement reason), and with a naked desire to harm rivals that relied on these tools (*i.e.*, a bad rival-injuring reason). So it will often be in practice.

Finally, there is a question of remedy. The idea that self-preferencing can be meaningfully "prohibited" supposes that platforms will be willing, or can be made, to directly subsidize competitive threats. But this will often be untrue. Suppose that we can correctly identify bad self-preferencing of both kinds (*i.e.*, Platform Moating and Platform Leveraging), and that we prohibit them when they happen. The problem is that it is not at all obvious whether the platform is likely to level up, benefiting consumers by extending the improvement to rivals' products, or level down, harming consumers further by withdrawing the improvements from its own products. In at least some of the most important cases, a platform may prefer not to make a product improvement if it would have to share it and thus to directly sponsor competitive threats to its own main cash cow. And if the improvement is already in place, it may simply be withdrawn or support may be terminated. Platforms may reasonably decline to invest in on-ramps for their rivals.

2. A Narrower Rule Could Address Harmful Self-Preferencing

The most promising cases for regulatory intervention on the grounds of dissimilar treatment probably involve specific acts of intentional, targeted, and unjustified impairment of particular rivals of the core platform monopoly: not merely rivals in the complementary market.

---

[39] *See* https://developer.apple.com/support/deprecated-sirikit-intent-domains.

For example, suppose that the operators of Google Search one day decided to banish Yelp from search results solely because it is a competitive threat to some aspect of Google's business. Or suppose that the operators of Twitter deactivated the functionality of links to rival microblogging networks and no other websites. Regardless of whether conduct like this is illegal, under most circumstances it does not serve consumers' interests.

We could imagine a category of high-risk denials. Such denials would be: *intentional* (in that they are not the incidental effect of a broader policy or policy change), *targeted* (in that they involve specifically targeting individual competitors, while leaving intact service to all non-targeted trading partners, rather than just preferring the platform's own business over third parties), *unjustified* (in that there are not supported by any procompetitive justification *other than* the proposition that a business is entitled to decline to affirmatively support its rivals), and *monopolizing* (in that they tend to increase monopoly power in a primary platform market).

It is not entirely clear that Congress would really want to try to prohibit even this, to the extent that antitrust does not already do so. Reasonable minds can differ about whether a business should be forced to actively subsidize its rivals, either individually or as a category. They might also differ regarding whether a business should be able to "price in" the fact that supporting a rival will bite into the business's own profits, and thus charge a profit-maximizing price that is higher than the platform charges to non-rival trading partners. One might reasonably fear that banning discrimination of this kind will lead to platforms keeping improvements for themselves that they would otherwise share with non-rival trading partners (*i.e.*, self-preferencing as an alternative to targeted discrimination against rivals). One might also fear pushing courts and agencies into figuring out whether a platform had unlawfully discriminated against rivals by providing

inadequate assistance, too-limited connectivity, insufficiently rapid service and support, insufficiently prominent promotion, and so on.

But, even with all that said, it is clear that the balance of harms and benefits of a ban on intentional, targeted, and unjustified discrimination amounting to monopolization against actual or potential rivals tips differently from the case of self-preferencing. And if Congress desires to protect against this threat, then it can do so with a much narrower rule.

Reasonable minds can differ here: my own instinct is that Congress should probably not create even this much narrower rule. I think naked discrimination of this kind is pretty rare, and the close cases that will emerge in practice will present all the challenges and concerns described above, including the risk of punishing product improvements. Nor do I think there is a principled basis for creating a different rule in the context of digital platforms, when this phenomenon is common to the entire economy. I also think there is room to apply Section 2 of the Sherman Act to at least some such practices, including when an anticompetitive condition is used to deter entry or expansion. But a rule of this kind would surely be *much* better than a general rule against self-preferencing, and I could imagine it doing helpful work in some of the most troubling cases.

E. AICOA's Qualifying Provisions Do Not Resolve Concerns

1. The Harm to Competition Criterion Is Likely to Be Ineffective

The current draft of AICOA prohibits self-preferencing if conducted in a manner that "would materially harm competition," and creates an affirmative defense to other violations if a defendant can establish that the conduct would *not* result in "material harm to competition."[40]

[40] AICOA (May 2022 draft), Section 3(a)(1), 3(a)(2), 3(b)(2).

I do not think this language resolves the concerns identified above. To be sure, it is much better to include this language than not to do so! It could be understood as a reference to antitrust's concept of an anticompetitive effect or tendency that injures welfare: that is, increased prices, reduced output, reduced quality, etc. If this is its purpose, AICOA should explicitly say so.

But there are two problems.

The first is that "harm to competition" is just not a phrase with a single self-executing meaning. It *could* be interpreted to mean welfare harm in a manner we would associate with traditional antitrust; or it could be interpreted to mean "injury to rivals," This reading would be more than plausible, given that AICOA is not an antitrust statute, that "harm to competition" is not a phrase that appears in the antitrust statutes (unlike, say, "where . . . the effect . . . may be substantially to lessen competition") and that it makes no reference to a principle of consistent interpretation. And if the latter, it is no kind of limit at all.

The failure to take an explicit view on this is a serious and glaring problem with the current draft. It creates profound ambiguity at the heart of the bill. At all costs, the provision should be defined: either it's a consumer-welfare test, or it's an injury-to-rivals test. It cannot be both.

Many distinguished commentators have made this point. For example, Professor Doug Melamed—former acting head of the DOJ Antitrust Division under President Clinton—has noted:

> Plaintiffs will no doubt argue, and courts might agree, that Congress did not intend to incorporate existing antitrust concepts and that "harm to competition" means any reduction in competition by, for example, causing a weak and insignificant rival to exit from an intensely competitive market. Plaintiffs will argue that Congress could have specified that the bill incorporates the antitrust notion of injury to competition but that Congress chose not to do that, and they will emphasize that the whole point of the bill was to supplement the antitrust laws with stronger prohibitions.

> The bill could be very harmful if it is construed to require, not increased market power, but simply harm to rivals. The U.S. has in the past tried laws that insulate weak firms from competition provided by more efficient firms. The results have been increased costs, reduced output, and harm to consumers and suppliers.[41]

And Professor Herbert Hovenkamp has made the same point:

> If competition is defined in an economically sensible way to refer to reduced market output and higher prices, then the statute might end up limiting its reach to conduct posing a realistic threat of competitive harm. If it means something else, such as merely injuring a rival or placing it at a disadvantage on that particular platform as opposed to the market as a whole, then it could end up doing a great deal of harm. . . . If the AICOA is redrafted, this provision more than any other needs clarification. Is its principal purpose to protect competitors, without regard for market output, prices, innovation or other indicia of consumer harm? Or is the statute intended to promote the antitrust function of ensuring that markets are competitive?[42]

Second, in forced sharing cases, as I read it, the "harm to competition" test invites application against the wrong baseline *even if it is understood in the sense of welfare harm*. It implicates a well-known fallacy in the law of refusal to deal. On the most natural reading of the text, the "harm to competition" seems to be measured against a world in which the relevant preference (or access, or interoperability, or search ranking) is extended to all third parties. In other words, a court or agency is invited to see that some benefit (say, a low price, or a product improvement) is being conferred on an internal trading partner, and is then asked to consider whether competition would be materially improved if that benefit were provided on equal terms to all. *But the answer to that question will virtually always be yes.* Through an *ex post* lens, it maximizes short-run competition to require that investments already created be shared at marginal cost.

---

[41] A. Douglas Melamed, *Why I Think Congress Should Not Enact the American Innovation and Choice Online Act*, Comp. Pol'y Int'l (June 19, 2022), https://www.competitionpolicyinternational.com/why-i-think-congress-should-not-enact-the-american-innovation-and-choice-online-act.

[42] Herbert Hovenkamp, *Gatekeeper Competition Policy* (Feb. 2023) 23–24, https://ssrn.com/abstract=4347768.

The inference of competitive harm is fallacious because it misses the *ex ante* question. In a great many cases, the product improvement would never have been made if the government was going to come along and compel universal sharing, with all its burdens.[43] It always looks *short-run* procompetitive, after the fact, to compel sharing at marginal cost (which may be at or near zero) to maximize output. But doing so would often inflict serious harm on incentives to invest.[44]

Nor is it obvious how the court is supposed to assess the *long run* question that includes the *ex ante* perspective. Is the court supposed to ask whether this platform would have introduced this feature if it had known that equal access would be mandated after the fact? Whether other future investors will be chilled by an imposition of liability? How is an agency or court supposed to balance this in practice? If a court is supposed to do this kind of ex ante analysis, AICOA should state that clearly, and provide some kind of guidance on how it is to be done.

To sum up: I fear that the harm to competition requirement will collapse into simply asking whether the innovation is valuable to the third party seeking access, and whether static welfare will be improved in the short run by forced sharing. If so, then it will be a rubber stamp. And if the intention is to have a court or agency decide whether the self-preferencing plays a reasonably

---

[43] *See, e.g.*, Howard A. Shelanski, *Unilateral Refusals to Deal in Intellectual and Other Property*, 76 Antitrust L.J. 369 (2009).

[44] *See, e.g.*, Jorge Padilla, Douglas H. Ginsburg & Koren W. Wong-Ervin, *Antitrust Analysis Involving Intellectual Property and Standards: Implications from Economics*, 33 Harv. J. L. & Tech. 1, 8, 10 (2019) ("After an [intellectual property right] has been created, it is often most efficient to make it widely available — full dissemination and disclosure of an innovation is socially optimal ex post. But if dissemination or disclosure is made mandatory, then the incentives are likely not there to create [intellectual property] in the first place. As such, ex ante, the ability to exclude and limit dissemination and disclosure is socially optimal. In other words, the core right to exclude is often critical to induce innovators to invest in costly and risky R&D. . . . [O]ne can imagine the value that society loses when pharmaceutical companies charge prices for pills that far exceed the cost of manufacturing those pills. But . . . this . . . examines only the static view of monopoly pricing, and ignores the dynamic view."); Glen O. Robinson, *On Refusing to Deal with Rivals*, 87 Cornell L. Rev. 1177, 1191–92 (2002) ("Surely it cannot be enough for a firm to assert that it would be desirable for them to use their competitor's property and then shift the burden to the competitor to prove that the suggested arrangement is not efficient. . . . When a Wal-Mart comes to town, it is a safe bet that many smaller retailers that sell similar merchandise will suffer. Those who think that small retailing serves a vital community function may lament this new competition, but sensible people are unlikely to propose the remedy of forcing Wal-Mart to provide floor space to its smaller competitors so that they may enjoy the benefits of Wal-Mart's magnetic pull on consumers. Turning Wal-Mart into a wholesaler of retail space . . . would be a counterproductive strategy if competition is what we are seeking.").

important role in incentivizing the platform to introduce, maintain, or improve the feature in question, then at a minimum that should be directly stated, and some guidance given to an agency or court attempting to apply that test. And Congress should understand that this will considerably narrow the scope of any self-preferencing prohibition.

2. AICOA's General Affirmative Defense Is Too Narrow and Too Demanding

The current draft of AICOA creates a general affirmative defense against core self-preferencing as well as all the other violations established in Section 3(a)(3)–(10). A defendant establishes this defense if it establishes that the conduct is "reasonably tailored and reasonably necessary"—such that the objective "could not be achieved through materially less discriminatory means"—to: (A) prevent a violation of, or comply with, law; (B) protect "safety, user privacy, the security of nonpublic data, or the security of the covered platform"; or (C) "maintain or substantially enhance the core functionality of the platform."[45] An exception to the definition of "business user" also excludes entities that are a "clear national security risk."[46]

This provision aims at a good purpose: to prevent AICOA from biting on conduct that is justified. The problem is that this provision is likely to be all that stands between a platform and liability for a *product improvement* (!) or other commonplace beneficial behavior, and it is much too weak a shield to do that work. I have four main concerns.

a) The Less Discriminatory Alternative Test Seriously Weakens the Defense

First, this defense is unlikely to be much help at all in many cases, because it requires the defendant covered platform to show that the conduct in question "could not be achieved through

[45] AICOA (May 2022 draft), Section 3(b)(1).

[46] AICOA (May 2022 draft), Section 2(a)(2).

materially less discriminatory means." It does not seem to matter that the platform *would not rationally* have gone to the burdens and expense of, say, sharing an improvement or feature innovation with the whole world, including because doing so would have been very costly or risky or otherwise unappealing or implausible. If it "could" have been done in a non-discriminatory way, then there's no defense *even if* the effect of the challenged conduct is clearly good for consumers.

For example, suppose that a covered platform preinstalls an app or integrates a function. A rival complains that this is unlawful self-preferencing in violation of Sections 3(a)(1) and 3(a)(2). The platform responds that this is a "core" product improvement under Section 3(b)(1). *But now the rival responds that the defense does not apply because there was a less discriminatory alternative: namely, preinstalling or integrating the rivals' app too!* So the defense hangs by a thread: unless the covered platform can affirmatively show that it was not (technically? commercially? conceivably?) possible to preinstall or integrate the rival's product, the defense is no help. The fact that it would have been very expensive, or very time-consuming, or very difficult, or just unprofitable to do it in a less discriminatory way, seems to be no help.

b) The Defense Omits Many Important Justifications

Second, by specifying a narrow set of grounds that may justify self-preferencing, the defense offers no protection for denials that—surely!—ought to be protected. For example, the defense does not appear to protect a platform that declines to give equal treatment to a product, service, or entity for reasons of:

- objectionable content (*e.g.*, sexually explicit content—including in products, services, or apps aimed at or marketed to children; promotion of terrorism; promotion of violence or criminality)[47];
- inaccurate, false, or outdated information;
- poor quality service or a bad, buggy product;
- spam (*i.e.*, objectionable, intrusive, and unwelcome advertising or valueless content);
- fraud, deception, and exploitation;
- threat of consumer confusion;
- threat to the security of *other* ecosystem participants (not the platform itself);
- law enforcement or national-security concerns that do not involve an entity that has already been specifically designated by the federal government as subject to sanctions or as a "national security, intelligence, or law enforcement risk[]"[48] and which do not rise to the level of a "clear" national security risk[49];
- unusual technological, commercial, or other difficulties or costs of integration; or
- lack of information regarding, or ability to investigate, a possible concern (*e.g.*, the ultimate ownership and control of an app, or the way in which an app will use data).

And if the existing terms "safety, user privacy, the security of nonpublic data, or the security of the covered platform" are intended to cover some of the foregoing grounds, that should be made clear.

---

[47] As I note below, it is not clear to me how the First Amendment or Section 230 is intended to interact with the prohibitions in Section 3(a), nor what the optimal relationship would be. *See infra* II.F.1.

[48] AICOA (May 2022 draft), Section 3(c)(8)(A)((iii).

[49] AICOA (May 2022 draft), Section 2(a)(2).

c) The "Core" Limitation Is Undesirable

Third, by limiting the platform-enhancement defense to "core" functionality, the defense does not protect even a clear product improvement that merely enhances *non-core* functionality. Strikingly, the term "core" is not defined, and there does not appear to be any very good way to tell what it means even directionally. Does it improve the "core" functionality of an app store to add or promote an app? Does it improve the "core" functionality of Windows to include a media player or a word processing app? Why would the defense not extend to *any* mere functionality improvement, whether the improved function was core or not? Does the introduction, integration, or improvement of a product, service, app, or function count as the improvement of the "core functionality" of a platform? How can we tell? Moreover: is the "maintain or enhance" test applied against a counterfactual in which the platform does not implement the improvement at all, or one in which it shares it with all third parties? (If the latter, it will invite the same *ex post* fallacy described above.) And is the word "substantially" in "substantially enhance" intended to do any limiting work: and, if not, why is it included?

There does not seem to be any good reason for limiting this defense to "core" functions, however defined. The "core" test should almost certainly be removed: any measure reasonably related to the maintenance or improvement of a function should not be an AICOA violation.

d) Fact-Intensive Defenses Are Likely to Be Little Comfort

Fourth, the defenses are likely to be heavily fact-intensive, and the burden is with the platform to prove that they justify a denial by a preponderance of the evidence.[50] This means that

[50] AICOA (May 2022 draft), Section 3(b)(4).

if the platform has grounds for concern, but cannot ultimately prove those grounds on a preponderance of evidence, there will be no defense. And if a platform *fears* that it cannot do so, or does not want to face the expense of doing so, then the defense will not help it in the first place.

For all these reasons, I fear that the general affirmative defense will be a paper shield in practice. Given the breadth of AICOA's basic prohibitions, and the number and variety of things that those prohibitions will catch that they should not, the general affirmative defense in Section 3(b)(1) is far too narrow and weak to allay my concerns regarding the bill.

F. Other 3(a) Provisions Raise Numerous Concerns

Although my focus has been on the core self-preferencing rules, because I take these to be the central thrust of AICOA, the bill also creates an array of other rules. These also present a series of risks to consumers and others. The following discussion illustrates some of those concerns.

1. The TOS Discrimination Ban Harms Consumers and Implicates Content Moderation (Section 3(a)(3))

Section 3(a)(3) prohibits a covered platform from "discriminat[ing] in the application or enforcement of the terms of service of the covered platform among similarly situated business users in a manner that would materially harm competition." This is similar in thrust to the rule against self-preferencing, but it involves the preferencing of *third parties* other than the platform itself, and it takes place within the four corners of the platform's "terms of service."

As a threshold matter, it is not quite clear what useful work "terms of service" is doing or why discrimination within the terms of service should be treated differently from those outside those terms. The phrase "terms of service" is not defined. The rule would seem to treat identical

practices differently depending on whether they fall within what the platform has chosen to designate "terms of service." That does not seem like the right outcome!

That issue aside, a general non-discrimination obligation inflicts consumer harms by preventing platforms from offering good terms when they could or would not do so across the board. For example, suppose that a covered platform is able and willing to offer a high-volume, high-quality trading partner some kind of benefit, such as low fees, cooperation on a new product feature, or inclusion in a "trusted partner" program of some kind. Those are efficient and desirable things! But the risk of liability simply deters the platform from doing so. (This is the classic problem that causes the Robinson-Patman Act to hurt consumers.[51])

Of course, there are circumstances under which it might be appropriate to impose a non-discrimination obligation in a particular market for a particular reason. Usually these involve a policy decision that competition cannot take place and that a regulated monopoly is, exceptionally, the next-best alternative. But that determination is generally made on a market-by-market basis, and in full awareness of the costs and risks. Applying it across the board to all practices by covered platforms does not even arguably fit this description.[52]

Separately: it is not at all clear to me how this provision is intended to interact with the practice of content moderation (including banning, blocking, and ranking), the law of the First

---

[51] *See generally, e.g.*, Herbert Hovenkamp, *Antitrust Modernization Commission: Written Testimony on the Robinson-Patman Act* (July 2, 2005), https://govinfo.library.unt.edu/amc/commission_hearings/pdf/Hovenkamp.pdf.

[52] The customary case for public-utility-style regulation does not seem a very promising fit with most digital markets. Network effects may reward scale, but real competition is often sustainable given the presence of product and service differentiation, ad-supported platform services, multihoming, and the fact that users can connect to new and existing rivals. Uber can co-exist with Lyft; Amazon with Walmart, Target, eBay, and Etsy; Google with Bing; Apple's iPhone with Google's Android; Microsoft Windows with Mac OS; Microsoft Word with Google Docs; and so on. Of course, market power and monopoly are still possible and a serious concern, here as elsewhere in the economy. My point is that there is no reason to give up on competition and embrace the sedentary model of regulated monopoly.

Amendment, Section 230, or the control of spam or content that might be thought objectionable (*e.g.*, sexually explicit material, or the promotion of terrorism or violence).[53] The text of Section 3(a)(3) strongly hints that content moderation will be a violation, assuming that content moderation involves applying or enforcing terms of service. At a minimum, some such practices seem to fall within Section 3(a)(3). As a result, Section 3(a)(3) is mostly naturally read to require that any moderation be non-discriminatory (*i.e.*, not disadvantage "similarly situated" business users).

If some content moderation practice is, or is held to be, discriminatory among similarly situated business users, and if the harm to competition criterion is satisfied (more than plausible if the covered platform is an important input to or distributor of content in the relevant market), then a presumptive violation is established. And, as noted above, control of spam or objectionable content is *not* a basis for the affirmative defense. I have no idea at all whether the First Amendment, Section 230, or anything else would protect a platform in such a case.

The concrete case might look something like the following. A business user of a covered platform generates content that is controversial: regarded by some as spam or irresponsible falsehood, and by others as important political speech. Or perhaps a business user generates sexually explicit content. A covered platform suppresses or removes the business user's website, posts, content, or account. The business user complains—to a federal enforcer or a State Attorney General—that this constitutes discrimination because other businesses are not being treated in the same way. And it claims harm to competition because distribution on the platform is competitively important in the market in which the business user competes. The enforcer agrees and brings an

[53] *See, e.g.*, Free Press, Provision in Senate Antitrust Bill Would Undermine the Fight Against Online Hate and Disinformation (Jan. 20, 2022), https://www.freepress.net/news/press-releases/provision-senate-antitrust-bill-would-undermine-fight-against-online-hate-and-disinformation (Section 3(a)(3) "would make it difficult or impossible for covered companies to deplatform and remove from their sites any business that traffics in hateful, racist, violent or otherwise harmful content").

action under AICOA as a Section 3(a)(3) violation. And now the platform does not seem to have access to the affirmative defense. Everything will then turn, I think, on: (1) what "similarly situated" means (is *any* discrimination allowed as long as the platform can articulate a reason? How is a court to tell what constitutes a "good" or "bad" reason, or a relevant similarity, under Section 3(a)(3) of AICOA?); and (2) whether other laws, such as the First Amendment or Section 230, would apply. It is not at all clear what the drafters of AICOA intend.

Reasonable minds may feel differently about the optimal rule here. So, too, may reasonable federal enforcers, and reasonable State Attorneys-General, empowered to enforce AICOA. To avoid serious confusion and divergent enforcement, Congress may wish to clarify the intended operation of these rules. It is worth remembering that spam, in particular, confronts every digital platform that allows users and businesses to create and share content.[54]

2. The Access and Interoperability Mandates Threaten Users (Section 3(a)(4))

Section 3(a)(4) imposes a strikingly broad duty of forced access and interoperability. All business users must be accorded equal "access" and "interopera[bility]" to "the same platform, operating system, or hardware or software features that are available to the [platform's competing or potentially competing] products, services, or lines of business . . . except where such access would lead to a significant cybersecurity risk[.]"

[54] *See, e.g.*, Mike Masnick, *Very, Very Little Of 'Content Moderation' Has Anything To Do With Politics* (May 25, 2022), https://www.techdirt.com/2022/05/25/very-very-little-of-content-moderation-has-anything-to-do-with-politics/ (noting, for example, that more than half of Facebook's content moderation in Q4 2022 related to spam, and most of the other half related to fake accounts).

As a threshold matter, this provision centrally rests on the terms "access" and "interoperate" which are, rather strikingly, not defined by the bill. Figuring out what these terms mean will be a time-consuming and expensive task for businesses, agencies, and courts.

Moreover, on most plausible readings, this obligation seems to require handing over the keys to a platform, device, or ecosystem to a really striking extent, with only the final proviso for very limited comfort.[55] For example, Apple has "access" to an iPhone's camera, microphone, GPS locator, and so on, as well as tremendous data regarding users and their behavior. This provision seems to presumptively require Apple to fork over whatever hardware access is used by a product like the phone function, Apple Maps, or Apple's mail software to any manufacturer of a competing app. (Nor is it obvious what a "software feature" is. Is information about consumer behavior, preferences, or location a "software feature"? What about an algorithm applied to such data?)

The premise seems to be that if consumers are willing to trust, say, Apple with access to the phone hardware, then they must be willing to trust any conceivable supplier of a third-party app, peripheral, service, or product. I think this is misconceived, and that it misses a critical "trust gap" that often will separate a known and trusted platform owner from an unknown and untrusted

[55] Others have made this point. *See, e.g.*, Mark Jamison, Congress Could Weaken U.S. Competitiveness with These Two Bills, AEI (Aug. 21, 2022), https://www.aei.org/op-eds/congress-could-weaken-u-s-competitiveness-with-these-two-bills/ ("Given the platforms' regulatory hurdles and delays, it is likely that the Russian actors could have planted malware designed to stealthily collect U.S. and Ukraine metadata, steal software, intercept and alter data flows, surveil Americans and Ukrainians, disrupt the platforms' attempts to prevent misuse, and compromise platform functions. The regulations would also have required the U.S. platforms to provide data to a wide range of stealth Russian-supported companies. American lives and interests would have been put at risk, as would the lives and interests of American allies."); Krisztian Katona, *AICOA's Data Security, Privacy, and Content Moderation Issues Call for Risk Assessment* (June 7, 2022), https://www.project-disco.org/privacy/060722-aicoas-data-security-privacy-and-content-moderation-issues-call-for-risk-assessment/ ("Complying with this requirement to grant access to any platform, OS, hardware, or feature means giving unfettered access to any putative competitor. Leading cloud services would seemingly need to grant access to back-end infrastructure and physical hardware–the same infrastructure and hardware that supports essential sectors like healthcare, energy, and banking and finance, to say nothing of state and federal governments. Similarly, device manufactures regularly restrict access to APIs that grant full read/write access to the device–that is necessary to perform backups but can easily be abused in ransomware attacks–or that grant access to sensitive information like health data or mobile payments. These private APIs keep sensitive data and permissions secure and opening them up to all comers represents a major privacy and security risk.").

third party supplier. Many consumers may reasonably trust, say, Apple or Amazon, without equally trusting every third-party app developer or goods seller that happens to be on the platform. Doubly so if the government is going to come along and *force* app developers and goods sellers onto the platform that the platform itself would have reasonably decided to keep out! And it is not at all clear to me what "interoperate" means.

The proviso at the end ("except where such access would lead to a significant cybersecurity risk," introduced in the May 2022 draft), seems to be a response to this glaring problem, but it is too vague and cursory to do that work. What is a "significant cybersecurity risk" and who must prove that access "would" lead to such a risk? The definition of "significant" and "cybersecurity" are critical but unexplained. Is this proviso intended to cover all undesirable uses of information, including not just those that involve criminal behavior or national security threats, but also uses that will expose users to spammy advertising, unwelcome contacts, or compromise their privacy? If so, that should be made very clear. Likewise, the relative burdens of proof of the plaintiff and defendant are critical. What if the platform merely has some grounds for concern and cannot or would not exhaustively investigate?

Nor are the legitimate concerns limited to cybersecurity. Forcing access to any "platform, operating system, or hardware or software features" is a dramatic incursion, with obvious implications for commercial confidentiality, platform integrity, and the platform's own resources. May a platform decline to provide such access on the ground that access of this kind would reveal competitively sensitive information, require expensive supervision, or threaten the efficient operation of the system? The answer appears to be no: that may not be a good idea.

3. The No-Conditioning Rule Is Vague and Threatens Ad-Supported Models (Section 3(a)(5))

Section 3(a)(5) bans certain conditioning practices. In particular, it prohibits a covered platform from conditioning "access to the covered platform or preferred status or placement on the covered platform on the purchase or use of other products or services offered by the covered platform operator that are not part of or intrinsic to the covered platform."

As a threshold matter, and importantly, it is not at all clear what "part of" or "intrinsic to" might mean here, in the context of an integrated platform with multiple features and functionalities. Those terms are not defined in the statute. (Nor, again, is "access.") This presents a difficult problem of interpretation: this provision purports to require unbundling of platform services but without any guidance as to what this would involve or how far it is supposed to go. Are Apple's App Store or In-App Payment mechanism "part of" or "intrinsic to" the iOS platform? Is iOS "intrinsic to" the iPhone or vice versa? Is Siri intrinsic to iOS? Are Amazon's warehousing or fulfilment services "part of" or "intrinsic to" the Amazon.com website? It is in the nature of software products of all kinds, and platforms in particular, to perform multiple functions. This provision seems to invite a landslide of uncertainty and miserably extended litigation: costs that will ultimately land on consumers. And it may just incentivize platforms to repackage two "separate products" into an integrated "single product," benefiting no-one.

That aside, this provision amounts to a *per se* rule against technological product tying of a kind that modern antitrust has long—and very wisely—left behind. Antitrust courts used to believe that "tying arrangements service hardly any purpose beyond the suppression of competition,"[56] but

[56] Standard Oil Co. of California v. United States, 337 U.S. 293, 305 (1949).

today virtually everyone agrees that supplying products together can often significantly benefit consumers and competition—even though tying can *also* sometimes cause harm. Above all, it makes no sense to automatically ban tying and integration among digital and software products, as the D.C. Circuit, sitting *en banc*, expressly recognized in the iconic pro-enforcement *Microsoft* decision:

> [T]here are strong reasons to doubt that the integration of additional software functionality into [a computer operating system] falls among [the category of *per se* illegal practices]. Applying *per se* analysis to such an amalgamation creates undue risks of error and of deterring welfare-enhancing innovation. . . . [J]udicial experience provides *little basis for believing that, because of their pernicious effect on competition and lack of any redeeming virtue, a software firm's decisions to sell multiple functionalities as a package should be conclusively presumed to be unreasonable and therefore illegal* without *elaborate inquiry* as to the precise harm they have caused or the business excuse for their use.[57]

The prohibition on conditioning also threatens free-to-use business models that allow non-ad-bearing apps or services to be provided free of charge through bundling with ad-supported apps. For example, a business may make and distribute an operating system for free because that operating system comes preloaded with apps that support monetization through advertising. It does not seem to be in the public interest to prohibit such business models.[58]

In addition, the prohibition also threatens to deny platforms the ability to reflect, in search rankings, the platform's knowledge of quality (and ability to guarantee it). For example, suppose that an e-commerce platform instituted a program pursuant to which it accorded greater prominence in search rankings to products for which it could directly guarantee stock and rapid fulfilment because it was, itself, providing warehousing and fulfilment services. This would direct consumers to products and services that the platform had reason to think were especially desirable.

---

[57] United States v. Microsoft Corp., 253 F.3d 34, 90–91 (D.C. Cir. 2001) (en banc) (emphasis added).

[58] *See supra* § II.C.3.

If this were prohibited on the ground that the platform was conditioning preferred status on buying its warehousing and fulfillment services, the result may not be in consumers' interests.

4. The Data Non-Use Obligation Prohibits Desirable Conduct (Section 3(a)(6))

Section 3(a)(6) bans a covered platform from using "nonpublic data . . . obtained from or generated on the covered platform by the activities of a business user or by the interaction of a covered platform user with the products or services of a business user to offer, or support the offering of, the products or services of the covered platform operator that compete or would compete with products or services offered by business users on the covered platform."

This prohibition directly prohibits platforms from better serving consumers. Virtually every business uses data generated by its activity—including, for appropriate businesses, activity that involves selling third-party products and services—to better understand and better satisfy consumer demand. An e-commerce platform uses information about what consumers do and do not want in order to better satisfy demand. A supermarket uses data about demand for products (including products manufactured by third parties); an auctioneer uses data about demand for goods (including goods to which it never takes title); a car dealer uses data about demand for cars (including those to which it never takes title); and so on. *Accurate information about demand allows businesses to compete better and more accurately, leaving consumers better off.*[59]

This provision ties platforms' hands to prevent third-party suppliers from facing "too much" competition, and consumers lose out as a consequence. It rests on the erroneous conclusion that data about, say, a merchant's sales on Amazon "belongs to" that merchant and does not

[59] Doug Melamed has made this point. A. Douglas Melamed, *Why I Think Congress Should Not Enact the American Innovation and Choice Online Act*, Comp. Pol'y Int'l (June 19, 2022), https://www.competitionpolicyinternational.com/why-i-think-congress-should-not-enact-the-american-innovation-and-choice-online-act.

"belong to" Amazon. It also prohibits platforms from buying data from business users for competitive purposes: but such a ban clearly harms competition and consumers.

To be sure, there are some very narrow circumstances where a data obligation may be anticompetitive, rather than procompetitive, but they do not involve the platform's access to information about its own activity. The most plausible version of this concern probably involves a platform agreeing to deal with a trading partner only so long as the trading partner commit to provide information or data relating to their own current or future competitive activity, to which the platform would not otherwise have access, and which would reduce the trading partner's incentive to invest in competition with the platform. Such a plan would usually violate the Sherman Act, and could safely be prohibited in the interests of consumers. As I note below, in the context of OAMA, I think such a prohibition could be framed by prohibiting a covered platform from making competitive use of competitively sensitive nonpublic business information *received directly from the third party* as a condition of operating a multisided platform or app store.[60] But the no-data rule in Section 3(a)(6) would reach *vastly* more broadly. It should be eliminated.

5. The "Access Own Data" Obligation Should Be Clarified (Section 3(a)(7))

Section 3(a)(7) prohibits a covered platform from "materially restrict[ing] or imped[ing] a business user from accessing data generated on the covered platform by the activities of the business user, or through an interaction of a covered platform user with the products or services of the business user, such as by establishing contractual or technical restrictions that prevent the portability by the business user to other systems or applications of the data of the business user."

[60] *See infra* § III.B.2.

It is hard to know what to make of this provision without a clearer sense of what it is supposed to require—and figuring that out across the many affected markets seems certain to involve extended uncertainty and expensive litigation. What exactly must be shared: simply information about the fact of a transaction? Identity of customers, including personal data of those customers? If, say, Apple has GPS information about where the consumer was when a purchase was made on an iPhone, or if Amazon has information about the search that led to a purchase, must information that be shared? If an advertiser buys an advertisement on a platform, does this provision allow the advertiser to obtain the identity of each user that viewed the ad (as that engagement was "generated by" the ad itself)? Is a content creator such as a video-maker on YouTube or a developer of a mobile game entitled to information about every user that downloads it? If a platform analyzes activity on its platform through a proprietary method, and by doing so gains valuable insights about consumer demand, must it share the results of that analysis with all the relevant third parties, on the ground that the analysis output is "data generated . . . by [their] activities"? And so on.

The point is not that transparency is bad: it can often be good. The point is that the nature of a desirable and workable obligation varies wildly from one market to the next. Indeed, an appropriately specific obligation to provide data or information, tailored to a specific market or set of markets in mind, could be procompetitive, as I note below.[61] Accordingly, I recommend Congress more precisely specify the meaning of this provision. I would support reasonably tailored transparency obligations in specific markets where the risks were low and the benefits clear.

[61] *See infra* § III.B.3., § IV.D.

6. The Free Uninstall, Free Default Rule Appears Dangerously Overbroad (Section 3(a)(8))

Section 3(a)(8) prohibits a covered platform from "materially restrict[ing] or imped[ing] covered platform users from uninstalling software applications that have been preinstalled on the covered platform or changing default settings that direct or steer covered platform users to products or services offered by the covered platform operator, unless necessary—(A) for the security or functioning of the covered platform; or (B) to prevent data from the covered platform operator or another business user from being transferred to the Government of the People's Republic of China or the government of another foreign adversary." Foreign adversary is defined, through Section 2(a)(8) and 47 U.S.C. § 1607(c), as "any foreign government or foreign nongovernment person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."

This provision prevents a platform from effectively hard-wiring certain software functions into the platform if the function is being executed by means of a separate "software application." This may not lead to logical results, because it does not affect the platform's ability to including multiple functions in a single product or service. Thus, for example, it would appear to presumptively prevent Microsoft from making the Edge browser a non-uninstallable "application," but would not prevent Microsoft from making browser functionality an integral part of the Windows operating system. It is not obvious whose interests are protected by encouraging a platform operator to spend time and money re-combining products and services in a slightly different way.

It is also not clear what the prohibition on inflexible "default settings" is intended to accomplish, outside what I take to be easy cases (*e.g.*, a default search provider for address-bar search). Every feature and function on a covered platform works a certain way: is AICOA really intended to apply to treat these as "defaults" and require that consumers be able to choose third-party options for any function? Or is something a default *only* if the platform owner builds in an option to switch to a third party in the first place? If so, this rule may just encourage platforms to eliminate the option and make everything an integrated function rather than a menu with a default.

Also unclear is a simpler issue: what does this provision actually require? What is the obligation of a platform with respect to email defaults on an iPhone, search defaults on a browser bar, camera apps on an operating system, mapping apps on search results, transaction handling software on any platform? What is a platform required to do: create a default menu that includes all known suppliers? Accept and review applications and screen them for quality? Must some kind of appeal be provided? What if adding a third party to the list requires something sensitive: for example, a mapping app requires location information, a camera app requires access to the camera, a transaction handling app requires credit card information. It is not remotely clear what is contemplated, permitted, or prohibited.

The purpose of the final condition seems to be to allow businesses to prevent a user (or an intermediary like a device original equipment manufacturer) from changing defaults to point to a service owned or controlled by the PRC or "another foreign adversary." But how is the platform owner to know what services are in fact under the thumb of an entity that qualifies as a foreign adversary? Digital services and products offered by a foreign power are unlikely to prominently identify themselves. Also, what about hostile and malicious actors here at home?

In practice, it is not at all clear how a platform is supposed to be able to protect against a user—or an intermediary like a device manufacturer or a retailer, whether knowingly or otherwise—redirecting a default or other function to point to a service that is terribly unsafe or unsound. Forcing a platform to allow a GPS mapping function, search function, camera function, or mail function to be reassigned to Russian Hacker Maps, Russian Hacker Search, Russian Hacker Video Sharing, or Russian Hacker Email does not seem like a step forward for the American consumer: even if those apps are masquerading under the name "USA Trusty Maps" and so on. And the same is true of Domestic Hacker Maps!

Nor is it clear why this limitation is confined to the "government" of foreign adversaries. Is the intention really to force platforms to grant equal access to privately owned entities—whether or not they are provably state-influenced—established in foreign adversary nations? And, finally, the vagueness of the "foreign adversary" definition in 47 U.S.C. § 1607 leaves a covered platform in an uncomfortable position of figuring out whether an agency or court will agree that a particular country is "engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons."

7. The UX / Search Preferencing Ban Replicates the Harms Described Above (Section 3(a)(9))

Section 3(a)(9) prohibits a covered platform from, "in connection with any covered platform user interface, including search or ranking functionality offered by the covered platform, treat[ing] the products, services, or lines of business of the covered platform operator more favorably relative to those of another business user and in a manner that is inconsistent with the neutral, fair, and nondiscriminatory treatment of all business users[.]"

This is a version of the general self-preferencing ban, but it lacks the harm to competition criterion, and is subject to the second of AICOA's affirmative defenses. My comments regarding this provision accordingly duplicate those above regarding self-preferencing, except to note that it is very broad. It forbids self-preferencing with respect to any user interface including, but not limited to, search rankings: thus, Amazon could not specially promote Amazon Studios at the top of its own page; Apple could not specially promote Apple+ content on its page, and so on. It would accordingly prohibit much product improvement and integration, including special promotions in connection with new market entry, and many page-design choices.

Moreover, to the extent that this provision also introduces the concepts of "neutrality" and "fairness," I suggest removing those provisions or defining them very clearly. It is notoriously difficult to assign anything like a consensus meaning to these two concepts, and AICOA surely does not need to import those difficulties. It is not clear that there is any such thing as a "neutral" or "fair" search ranking or user interface design.

I separately note that this provision, like Section 3(a)(3), presents the issue of content moderation. Among other things, the First Amendment appears to be implicated by government supervision of what a platform publishes and promotes: regulating web page design and search-result presentation may neither be wise nor Constitutional.[62] As I note above, AICOA's

[62] *See, e.g.*, Zhang v. Baidu.com, Inc., 10 F. Supp. 3d 433, 435 (S.D.N.Y. 2014) ("[T]he First Amendment protects as speech the results produced by an Internet search engine."); e-ventures Worldwide, LLC v. Google, Inc., Case No. 214-CV-646, 2017 WL 2210029, at *4 (M.D. Fla. Feb. 8, 2017) ("Google's actions in formulating rankings for its search engine and in determining whether certain websites are contrary to Google's guidelines and thereby subject to removal are the same as decisions by a newspaper editor regarding which content to publish, which article belongs on the front page, and which article is unworthy of publication. The First Amendment protects these decisions, whether they are fair or unfair, or motivated by profit or altruism."); *see also* Eugene Volokh & Donald M. Falk, *Google First Amendment Protection For Search Engine Search Results*, 8 J. L. Econ. & Pol'y 883 (2012).

relationship with the First Amendment, Section 230, and the law of content moderation is unclear, at least to me—I have no expertise at all in those areas of law—and could at least be clarified.[63]

8. The Anti-Retaliation Provision Is Desirable (Section 3(a)(10))

Section 3(a)(10) prohibits a covered platform from "retaliat[ing] against any business user or covered platform user that raises good-faith concerns with any law enforcement authority about actual or potential violations" of law.

This is a sensible provision. If AICOA is enacted, a provision of this kind is desirable.

9. AICOA's Supplementary Affirmative Defense Does Not Resolve Concerns

Section 3(b)(2) is an affirmative defense to conduct that would otherwise violate Section 3(a)(4)–(10). It is identical to the first affirmative defense, except that the defendant may also establish it by demonstrating, by a preponderance of the evidence, that the conduct has not resulted in and would not result in material harm to competition. In effect, this defense reflects the fact that harm to competition is *not* an element of the affirmative offenses in Sections 3(a)(4)–(10), but that lack of harm to competition can be shown by the defendant as a defense.

My reaction to this affirmative defense mirrors my reaction to the first affirmative defense, above.[64] Because I think the "harm to competition" test will amount to a rubber stamp for plaintiffs, I do not think that test will narrow the application of Sections 3(a)(1)–(3), and the fact that the burden is flipped to the defendant will make this even more of a problem than it is for Sections 3(a)(1)–(3).

---

[63] *See supra* § II.F.1.

[64] *See supra* § II.E.2.

In particular, I am concerned that the affirmative defense is subject to an unduly strict less-discriminatory alternative test that will wipe it out in many cases; is limited to improvements to "core" functionality, which is both narrow and undefined; fails to include many important policy grounds; and is heavily fact-dependent and requires the defendant to prove them by a preponderance of the evidence.[65] As a result, like the other affirmative defense, I expect that it will be a paper shield in practice.

G. Additional Comments

1. AICOA's New and Vague Terms Invite Endless Confusion and Litigation

AICOA introduces a forest of terms and concepts that are new, vague, and undefined, but which perform absolutely critical functions in defining the operation of the bill. To pick some specific examples:

- the definition of "business user" in Section 2(a)(2)(A), which is utterly foundational to AICOA's scope and reach, including the meaning of "use" and the scope of the status of being a "business user" for a company that is a business user with respect to one of its activities (if a business advertises on an internet website that can be found through Google, viewed on an iOS or Android device or a Windows PC, has it for that reason become a business user of Google, iOS, Android, and Windows? And if not, why not?);
- the scope of the exemption for "clear national security risk[s]" from the definition of "business user" in Section 2(a)(2)(B)(i), which will be a critical frontier of

[65] AICOA (May 2022 draft), Section 3(b)(4).

platforms' ability to protect national security (why must the risk be "clear" rather than "reasonable suspicion" or similar, and why are other forms of security threats not included?);

- the definition of "critical trading partner," including the definitions of the phrases "restrict or materially impede . . . access" of a (single?) business user to users or customers, or to a "tool or service . . [a] business user needs to effectively serve . . . users or customers," in Section 2(a)(6);
- the utterly central concept of "preference" in the signature prohibition in Section 3(a)(1) and elsewhere;
- the equally central concept of "material harm to competition" in Section 3[66];
- the definitions of "access" and "interoperate" in Section 3(a)(4), and of "materially restrict[ing], imped[ing], or unreasonably delay[ing]" access or interoperability, in Section 3(a)(4), which will define platforms' universal service obligations;
- the definition of "significant cybersecurity risk" in Section 3(a)(4), which is the ground on which denying access or interoperability will *not* constitute a presumptive violation;
- the terms "part of" and "intrinsic to," which define the scope of the rule against conditioning in Section 3(a)(5);
- the obligation to offer search rankings and user interfaces that are "neutral, fair, and nondiscriminatory" in Section 3(a)(9); and

[66] *See supra* § II.E.1 (explaining concerns).

- the scope of the critically important defense for "substantially enhanc[ing]" the "core functionality" of the platform in a way that "could not be achieved through materially less discriminatory means" in Section 3(b)(1), 3(b)(1)(C), which will be all that stands between a vast range of product improvements and liability.

The combination of the vagueness and the centrality of these and similar terms will put consumers, businesses, agencies, and courts in the unhappy situation of having to make this large and complicated plane while it is in the air. Antitrust doctrine has wrestled painfully for almost 133 years with the concepts at the heart of Sections 1 and 2 of the Sherman Act ("restraint of trade" and "monopolize") and for almost 109 years with the operative test in Section 7 of the Clayton Act (whether the effect of a merger or acquisition "may be substantially to lessen competition or tend to create a monopoly"). Those terms remain battlegrounds today in antitrust. And there is virtually no agreement at all today—less than there has been in decades!—about what Section 5 of the FTC Act means when it empowers the FTC to prohibit "unfair methods of competition." But each of these pillars of antitrust is pretty brief and concise.

AICOA will introduce a swathe of new, undefined, but critically important terms into competition enforcement and compliance, which will impact a vast number of negotiations and commercial activities throughout our economy (including in some of our most valuable and innovative markets). For the most part, the terms identified above do not exist in antitrust doctrine. And for those that seem to nod at an antitrust-like meaning—"harm to competition" is a prominent example—AICOA very pointedly does *not* clarify whether it is intended to adopt a consumer-welfare definition from antitrust, or different standards of its own, such as an injury-to-rivals standard. The resulting uncertainty, counseling and litigation costs, will delight only the lawyers,

and the businesses that can successfully use the threat of those costs to extract negotiating concessions. Those resources are surely better spent supporting antitrust enforcement, leveraging more than a century of investment, rather than beginning again from the ground up.

2. AICOA's Scope Appears Arbitrary

a) The "Covered Platform" Definition Does Not Seem Principled

I take Sections 2(a)(5)–(6) to define a "covered platform" as an "online platform" (as defined in Section 2(a)(9), discussed in the next section) that:

1. **has many US users**, by having, during a relevant 12-month period, *either* 50 million monthly active US-based users *or* 100,000 monthly active US-based business users (even if these thresholds are satisfied only for a moment);

and

2. **satisfies a bigness test by sales, market capitalization, or worldwide user base**, through:
   a. being owned or controlled at any point during a relevant two-year period (apparently even if that person no longer owns or controls the relevant platform?) by a person with net annual sales of $550 billion, *or*
   b. having an average market capitalization above $550 billion for a 180-day period during a relevant two-year period; *or*
   c. having at least one billion worldwide monthly active users at any point during a relevant 12-month period;

and

3. **is a "critical trading partner"** for the sale or provision of any product or service offered on or directly related to the online platform, through being "a person that has the ability to restrict or materially impede the access" of:
   a. "a business user to the users or customers of the business user," *or*
   b. "a business user to a tool or service that the business user needs to effectively serve the users or customers of the business user."

This is a rather strained definition, and it gives the impression of arbitrariness. Specifically, it leaves a reader with the sense that it has been written to specifically target certain businesses. My understanding is that at this time,[67] it is likely to cover at least: Alphabet Inc. (Google) (270 million U.S. users[68]; market cap $1.15 trillion[69]); Amazon.com, Inc. (163.5 million U.S. Prime members[70]; market cap $965.6 billion[71]); Apple Inc. (125 million U.S. iPhone users[72]; market cap $2.33 trillion[73]); Meta Platforms Inc. (Facebook) (239 million U.S. users[74]; 2.9 billion monthly active users worldwide[75]); and Microsoft Corp. (market cap $1.86 trillion[76]; and no doubt there are more than 100,000 business users of Microsoft's platforms).

---

[67] Figures last checked February 28–March 2, 2023.

[68] Statista, Google - Statistics & Facts (Jan. 2023), https://www.statista.com/topics/1001/google/.

[69] https://finance.yahoo.com/quote/GOOG/.

[70] Statista, Number of Amazon Prime users in the United States from 2017 to 2021 with a forecast for 2022 to 2025 (June 2022), https://www.statista.com/statistics/504687/number-of-amazon-prime-subscription-households-usa/. Of course, the text relies on an inference that at least 1 in 3 Prime members is a monthly active user.

[71] https://finance.yahoo.com/quote/AMZN/.

[72] Statista, Number of iPhone users in the United States from 2012 to 2022 (Mar. 2022), https://www.statista.com/statistics/232790/forecast-of-apple-users-in-the-us/.

[73] https://finance.yahoo.com/quote/AAPL/.

[74] Statista, Number of Facebook users in the United States from 2018 to 2027 (June 2022), https://www.statista.com/statistics/408971/number-of-us-facebook-users/.

[75] Statista, Number of monthly active Facebook users worldwide as of 4th quarter 2022 (Feb. 2023), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

[76] https://finance.yahoo.com/quote/MSFT/.

Walmart.com (408 monthly active users[77]; market cap $383.3 billion[78]) approaches the threshold but does not appear to hit it. And it is not clear to me whether Visa Inc (> 300 million U.S. cards in circulation,[79] and surely more than 100,000 U.S. business users; more than 1.1 billion worldwide credit cards issued[80]; market cap $462 billion[81]); and Mastercard (> 319 million cardholders[82]; 992 million consumer credit cards issued, plus 122 million commercial cards (including credit and debit)[83]; market cap $333.9 billion[84]) qualify. (I understand that "payment" has been removed from the definition of online platform, but I'm not sure that this quite does it: are not Visa and Mastercard "online services" that "enable" the "sale" of goods within the meaning of the definition?) The Alibaba e-commerce platform (market cap $242.4 billion[85]) and the Tencent entertainment giant (>80 million Fortnite players[86]; market cap $449.6 billion[87]) do not appear to qualify.

It is important to appreciate what a departure AICOA would be for U.S. competition policy. I am not aware of any other instrument of U.S. competition policy that differentiates on the basis

[77] Statista, Worldwide visits to Walmart.com from December 2021 to May 2022 (June 2022), https://www.statista.com/statistics/714568/web-visits-to-walmartcom/.

[78] https://finance.yahoo.com/quote/WMT/.

[79] Statista, Largest credit card companies in the United States in 2019 and 2020, by number of active accounts (Nov. 2022), https://www.statista.com/statistics/605634/leading-credit-card-companies-usa-by-number-of-card-holders/; https://www.fool.com/the-ascent/research/credit-debit-card-market-share-network-issuer/.

[80] Visa Inc. Q1 2021 Operational Performance Data, https://s1.q4cdn.com/050606653/files/doc_financials/2021/q1/Visa-Inc.-Q1-2021-Operational-Performance-Data.pdf.

[81] https://finance.yahoo.com/quote/V/.

[82] Statista, Number of Mastercard credit cards in the United States and worldwide from the 2nd quarter of 2019 to 4th quarter of 2021 (Jan. 2022), https://www.statista.com/statistics/618137/number-of-mastercard-credit-cards-worldwide-by-region/.

[83] Mastercard 2022 Form 10-K, https://www.sec.gov/ix?doc=/Archives/edgar/data/1141391/000114139123000020/ma-20221231.htm, 7.

[84] https://finance.yahoo.com/quote/MA.

[85] https://finance.yahoo.com/quote/BABA/.

[86] Statista, https://www.statista.com/statistics/1238914/fortnite-mau/ (May 2020), https://www.statista.com/statistics/1238914/fortnite-mau/

[87] https://finance.yahoo.com/quote/TCEHY/

of market capitalization or other measure of bigness. Nor am I aware of any instrument of competition policy that has so many hallmarks of an effort to pick out specific businesses for special treatment. I think that our tradition is a point of pride for our legislative and regulatory practice: we do not pick winners and losers by name, or through criteria reverse-engineered with them in mind, nor do we single out politically unsuccessful businesses for special adverse treatment. I fear that breaking that tradition could have unhappy consequences. The unpopularity of the tech targets today may not break down along partisan lines, but with a little imagination one could imagine the same device being used in the future to target big businesses that have fallen out of favor with only one party, with AICOA cited as an example. That would be unfortunate.

Above all, it is not clear why the same regulatory response is appropriate for all the businesses that satisfy AICOA's thresholds and no others. For example, if the bill's concern is with durable monopoly power, why is there no requirement of durable monopoly power—or even market power—and no limitation to markets in which such power is present?[88] Why is the raw number of users or business users, annual sales, or market capitalization, relevant at all to the presence or absence of competitive concerns? If the concern is digital monopoly power, or digital platforms, why is the bill focused on a set of businesses that can be understood as having won the "last war," rather than others with monopoly power that may be smaller in absolute terms today but which enjoy considerable power in their respective markets? And what is the competitive concern that is common to the—very diverse—businesses that satisfy this definition, and not to

[88] As the ABA Antitrust Section observes: "[F]inding or designating a platform to be a 'covered platform' does not require or establish that it has market power in any relevant market. Size, in the sense of number of users or market capitalization, is not by itself evidence of market power. A firm may be large, as measured in these terms, yet lack the power to influence prices or exclude competitors." Comments of The American Bar Association Antitrust Law Section Regarding the American Innovation and Choice Online Act (S. 2992) Before the 117th Congress (Apr. 27, 2022), https://www.americanbar.org/content/dam/aba/administrative/antitrust_law/comments/at-comments/2022/comments-aico-act.pdf.

other businesses? What is the basis for thinking that the competitive concerns in e-commerce markets are the same as those in search markets, or mobile operating-system markets, or app-store markets, or social networking markets, and so on?

And if bigness is really the concern, why are other big enterprises in other areas of the economy not included? Tesla's market cap is $650.8 billion; NVIDIA's is $578.5 billion; UnitedHealth's is $444.7 billion.[89] They perform important work in markets, including high-tech markets, that matter to the U.S. economy. They are big! And their businesses could be understood in some respects as platforms: particularly Tesla and UnitedHealth. Why not include them too?

In addition, the definition of "critical trading partner" is strikingly broad and vague. It appears to encompass any business that offers a desirable means of reaching customers for even a single business user! In particular, the concepts of "restrict," "impede," "need," and "effectively" invite confusion and endless, agonizing litigation. Critical trading partner status seems just to mean "very valuable." Suppose, for example, that Amazon enables third-party merchants to do much better than they were doing before Amazon came along, or than they would be doing if Amazon did not exist. Has Amazon become, for that reason, something that the merchants "need[] to effectively serve [their] users or customers"? If so—and I assume the intention is that it would indeed satisfy the definition—then a "critical trading partner" just means a business that supplies a valuable service. This criterion is wholly disconnected from concerns with competition, anticompetitive practices, or market and monopoly power.[90]

---

[89] https://finance.yahoo.com/quote/TSLA/; https://finance.yahoo.com/quote/NVDA/; https://finance.yahoo.com/quote/UNH/.

[90] *See, e.g.*, Herbert Hovenkamp, *Gatekeeper Competition Policy* (Feb. 2023) 4, https://ssrn.com/abstract=4347768 ("[N[othing in the statute requires any showing that the covered firm's trade in the particular product under examination be dominant. For example, Amazon would very likely be designated a critical trading partner on the basis of its overall retail business. At that point its prohibitions would attach to its sale of, say, groceries, even though Amazon's share of the grocery market is a little over 1%. The same thing would apply to Microsoft's search engine Bing. While Microsoft is large enough to be a covered platform, and

The message that AICOA sends to other businesses that may, also, plan to invest in creating a valuable service is not an encouraging one. We should not encourage businesses to fear that they will succeed their way into regulatory punishment.

b) A Bigness Criterion Simply Invites Divestiture

Making the definition of a covered platform contingent on bigness suggests a reasonably easy path for any covered platform that believes, or finds, that it cannot run its business under the obligations of Section 3(a). Simply divide your business into two or three—along lines that cannot be predicted in advance and would have nothing to do with competition, and will do nothing to reduce monopoly or market power in any market—and carry on as before. I cannot see how this outcome would help anyone.

The underlying point is that bigness is not a proxy for competitive concerns or for monopoly power. This is one reason why antitrust has long avoided using size criteria, focusing instead on market and monopoly power in particular markets.

3. "Online Platform" Includes Things that Are Neither Online nor Platforms

Section 2(a)(9)(A) defines an online platform very broadly as "a website, online or mobile application, operating system, digital assistant, or online service that enables—(i) a user to generate or share content that can be viewed by other users on the platform or to interact with other content on the platform; (ii) the offering, advertising, sale, purchase, or shipping of products or services, including software applications, between and among consumers or businesses not

very likely a critical trading partner in its Windows operating system, Bing struggles in the search engine market, with a roughly 3% market share of consumer search. This failure to distinguish between the overall footprint of firms that operate platforms and the market shares of their products largely undermines the AICOA's value as a tool for improving competition.").

controlled by the platform operator; or (iii) user searches or queries that access or display a volume of information[.]" Section 2(a)(9)(B) excludes certain wire and radio services from the definition.

This definition of "online platform" embraces a startling range of products and services that would not ordinarily be called either platforms or even online! Specifically, it includes many businesses and services that are not multisided platforms: for example, a simple file storage folder could constitute a platform if it was a website or application that enables users to search or query information. So could a mobile application that contained an offline encyclopedia, or a library of audio or video materials that can be accessed through the web (audio and video materials are information too!). Nor must the service be "online" in the sense of "accessed via the internet": being a "mobile application," an "operating system," or a "digital assistant" is enough.

I assume that this is not a drafting error: that Congress indeed prefers not to limit the definition to multisided platform businesses or to services that are supplied in real-time on the internet. As a result, it may be better to re-label the term "digital service" rather than "online platform."

4. "Business User" Is Overbroad and Vague

Section 2(a)(2) defines a "business user" to include "a person that uses or is likely to use a covered platform for the advertising, sale, or provision of products or services." That person then appears to be a business user for *all* purposes. This is an exceptionally broad definition that may exceed what Congress has in mind. As I read it, it covers virtually every business that advertises on the internet or uses digital services. If I advertise on a website, and that website is accessible through Google and can be viewed on an iPhone, or a Windows PC, I seem to have become a business user of Google, iOS, and Windows with respect to all my lines of business. If I write my

advertising copy on Microsoft Office, I am a business user of Microsoft Office with respect to all my business lines. And so on. Surely that cannot be what Congress has in mind! As this demonstrates, the definition of "use" is critical—as is the scope of the status of being a "business user" (*i.e.*, whether my use of a covered platform as to *one* of my business lines makes me a "business user" as to all of my business lines).

Thus, for example, a landscaping business appears to constitute a "business user" of an iPhone and the iOS system because the landscaping services will be advertised or sold over websites, or even phone calls, viewed or conducted through the smartphone. Or a component supplier would be a "business user" of that same iPhone if it, too, advertised over internet websites that could be viewed through the iPhone: inviting the creative argument that the component supplier was the victim of self-preferencing if Apple decided to use its own components rather than those of the component supplier in the iPhone. Surely none of this is what Congress intends! The point is that vague definitions invite arguments of exactly this kind (as well as much closer and harder cases). When profits are at issue, such arguments will certainly proliferate and drown courts and agencies. Lawyers, not consumers, will benefit. The definition of "business user" should almost certainly be narrowed.

5. "Influence" May Be a Better Term than "Control"

Section 2(a)(4) effectively defines "control" at the 25% ownership level. But 25% seems an awfully low threshold for "control" as that term is traditionally understood: it is possible to satisfy this definition without being able to determine the competitive behavior of the "controlled" entity. Indeed, as many as four different entities can have "control" on this definition. Regardless of one's views on the core principles of AICOA, it may be worth revising this threshold upward

so that it more closely approaches "control" in the traditional sense, or just re-labeling it "material influence" to improve transparency.

6. The Possibility of FTC Rulemaking Is Unclear

Section 3(c)(1)(A) provides that the FTC shall enforce AICOA as it enforces Section 5 of the FTC Act. This raises the prospect that the FTC, at least under current leadership, may pursue AICOA rulemaking pursuant to purported powers under Section 6(g) of the FTC Act.

There is considerable doubt regarding whether Section 6(g) of the FTC Act authorizes rulemaking. For one thing, it is very far from clear that, if Congress had intended to create a broad unfair-methods rulemaking power, it would have done so through the following language:

> The Commission shall also have power—
>
> [. . .]
>
> (g) Classification of corporations; regulations
>
> From time to time classify corporations and (except as provided in section 57a(a)(2) of this title) to make rules and regulations for the purpose of carrying out the provisions of this subchapter.

For another thing, current Supreme Court guidance does not generally appear to favor the inference of broad or novel agency powers in broadly similar circumstances.[91] However, to avoid uncertainty regarding Congressional intent on the question of AICOA rulemaking, Congress may wish to make this clear in the institutional provisions of any version of AICOA that may be passed.

[91] *See* Alabama Ass'n of Realtors v. Dept. of Health and Human Servs., 141 S.Ct. 2485 (2021); West Virginia v. EPA, 142 S.Ct. 2587 (2022); *but see* Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672 (D.C. Cir. 1973) (upholding FTC rulemaking in a mixed competition / consumer protection case, albeit on grounds that are less widely accepted today).

7. The Interim Relief Provisions Are Too Generous

Section 3(c)(6)(C)(ii) provides that temporary injunctive relief may be awarded for a period of up to 120 days if "there is a plausible claim, supported by substantial evidence raising sufficiently serious questions going to the merits to make them fair ground for litigation, that a covered platform operator violated this Act; that the conduct alleged to violate this Act materially impairs the ability of business users to compete with the covered platform operator; and a temporary injunction would be in the public interest."

This is a specially *lowered*—that is, plaintiff-friendly—standard. As a general matter, the Supreme Court says that "A preliminary injunction is an extraordinary remedy never awarded as of right," and that "[i]n each case, courts must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief."[92] Specifically, the Court has instructed that: "A plaintiff seeking a preliminary injunction must establish that [1] he is likely to succeed on the merits, that [2] he is likely to suffer irreparable harm in the absence of preliminary relief, that [3] the balance of equities tips in his favor, and that [4] an injunction is in the public interest."[93] Lower courts routinely apply this instruction.[94] In the

[92] Winter v. Nat. Res. Def. Council, Inc., 555 U.S. 7, 24 (2008).

[93] Winter v. Nat. Res. Def. Council, Inc., 555 U.S. 7, 20 (2008).

[94] *See, e.g.*, H&R Block, Inc. v. Block, Inc., 58 F.4th 939, 946 (8th Cir. 2023) ("[A] party seeking a preliminary injunction must demonstrate: (1) the threat of irreparable harm; (2) the state of the balance between the harm and the injury granting an injunction will inflict on other parties; (3) the probability it will succeed on the merits; and (4) the public interest."); Commonwealth v. Biden, 57 F.4th 545, 550 (6th Cir. 2023) ("We consider four factors in determining whether a preliminary injunction should issue: (1) whether the moving party has shown a likelihood of success on the merits; (2) whether the moving party will be irreparably injured absent an injunction; (3) whether issuing an injunction will harm other parties to the litigation; and (4) whether an injunction is in the public interest."); Dream Defs. v. Governor of the State of Fla., 57 F.4th 879, 889 (11th Cir. 2023) ("A district court may grant a preliminary injunction only if the moving party shows: (1) "it has a substantial likelihood of success on the merits;" (2) "it will suffer an irreparable injury unless the injunction is granted;" (3) "the harm from the threatened injury outweighs the harm the injunction would cause the opposing party;" and (4) "the injunction would not be adverse to the public interest."); Singh v. Berger, 56 F.4th 88, 95 (D.C. Cir. 2022) ("A preliminary injunction is an extraordinary remedy that requires a moving party to make a "clear showing" that (1) it has a likelihood of success on the merits, (2) the balance of equities favors preliminary relief, (3) an injunction is in the public interest, and (4) it will likely suffer irreparable harm before the district court can resolve the merits of the case.").

Second Circuit, a party seeking a preliminary injunction must show: (1) irreparable harm *plus* (2) either (a) a substantial likelihood of success on the merits or (b) *both* sufficiently serious questions going to the merits *and* a balance of hardships that tips in the favor of the party seeking an injunction.[95]

But under AICOA a movant need only show that it is plausible—*not* likely—that there was a violation, a material impairment of ability to compete, and that an injunction is in the public interest. There is no irreparable harm requirement at all, and no consideration of the impact on the platform or associated equities or hardships. This is obviously a much more favorable standard for an injunction-seeker than even the Second Circuit's standard.

AICOA thus creates a specially lowered standard for preliminary injunctive relief, despite the Supreme Court's guidance. But it is not clear why this is remotely appropriate. Preliminary injunctive relief in an AICOA case will almost certainly involve forcing the platform to deal with some third party or category of third parties—including sharing data or access to digital infrastructure—and/or freezing the launch of some new innovation or feature, for up to four months. During this time, a competitor may steal a march to market on some new product generation in a product-improvement; a bad actor may obtain access to user data or commercially sensitive information; and so on. This seems undesirable.

---

[95] Ventura de Paulino v. New York City Dep't of Educ., 959 F.3d 519, 529 (2d Cir. 2020) ("Ordinarily, to obtain a preliminary injunction, the movant has to "show (a) irreparable harm and (b) either (1) likelihood of success on the merits or (2) sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly toward the party requesting the preliminary relief.""); New York ex rel. Schneiderman v. Actavis PLC, 787 F.3d 638, 650 (2d Cir. 2015) ("A party seeking a preliminary injunction must ordinarily establish (1) "irreparable harm"; (2) "either (a) a likelihood of success on the merits, or (b) sufficiently serious questions going to the merits of its claims to make them fair ground for litigation, plus a balance of the hardships tipping decidedly in favor of the moving party"; and (3) "that a preliminary injunction is in the public interest."), *see also* Citigroup Glob. Markets, Inc. v. VCG Special Opportunities Master Fund Ltd., 598 F.3d 30, 38 (2d Cir. 2010) (holding that this standard survives *Winter*).

It is worth considering the effect, not just of this interim-relief prohibition, but of its *threat* value in commercial negotiations. The prospect that an investigation will involve interim relief of this kind will be a powerful threat point for a third party bargaining with the platform, or even a government authority (such as a federal agency or State AG) earnestly but unwisely challenging reasonable conduct by the platform.

8. Forfeiture Is a Dramatic Remedy Given AICOA's Breadth

Section 3(c)(6)(D) provides that a "pattern or practice" of violating AICOA may result in forfeiture of a year's compensation by any appropriate corporate officer.

My main concern with this provision is that it will seriously exacerbate the risk that platforms will err on the side of favoring businesses (and their demands for access), over consumers (and their need for protection). AICOA already creates plenty of other reasons for a platform to fear that restricting third-party access will lead to plenty of hassles, costs, and business risks, even when there are reasonable grounds for concern and even when important consumer interests are hanging in the balance—as they often will be. But decisionmakers will become a *lot* more solicitous of third party interests when saying "no" instead of "yes" could result in the sacrifice of personal compensation.

I also fear that this provision is unduly punitive. To be sure: there may be cases in which forfeiture of compensation is an appropriate response to corporate wrongdoing. Clear and naked wrongdoing like fraud, bribery, flagrant and knowing violations of law seem to fall into this category. But—given the extraordinary breadth and vagueness of its terms, and the fact that a violation may involve nothing more than a product improvement—an AICOA violation is surely not one of them. Indeed, as currently written, it may be hard to find any major tech company that

is *not* engaged in a pattern or practice of violating AICOA! Moreover, it is very far from clear how to comply with the statute. Congress may not want to make a leadership role in a tech company a poisoned chalice in quite this fashion.

Accordingly, I would eliminate this provision.

9. The Limitations Period Is Unduly Long

Section 3(c)(7) provides for a six-year statute of limitations. This is strikingly long, above all for offenses that are so broadly and vaguely defined. Antitrust violations are subject to a four-year statute of limitations for challenges brought by injured persons and State Attorneys-General: something similar seems right for AICOA.[96]

10. The Exceptions Are Too Narrow

a) Intellectual property

Section 3(c)(8)(A)(i)–(ii) provides that nothing in Section 3(a) shall "require a covered platform operator to divulge or license any intellectual property, including any trade secrets, business secrets, or other confidential proprietary business processes, owned by or licensed to the covered platform operator," or "to prevent a covered platform operator from asserting its preexisting rights under intellectual property law to prevent the unauthorized use of any intellectual property owned by or duly licensed to the covered platform operator." Similarly, Section (c)(8)(B) protects actions that are "reasonably tailored to protect [certain copyright and trademark] rights of third parties." Thus, AICOA seems to create an absolute defense to a claim under Section 3(a) if

[96] 15 U.S.C. § 15b.

equal treatment (or other compliance) would necessarily involve an IP license, or if the action is reasonably tailored to protect certain third-party IP rights.

This is welcome to the extent that it helps to narrow the broad reaches of Section 3(a). But it creates a very sharp disconnect between IP rights, which are specially protected under AICOA, and all other property and contract rights, which are subject to enforced sharing under Section 3(a). It is not obvious why this disconnect is appropriate, or why AICOA does not reflect similar concerns about forced sharing outside the IP context.

b) Federal government blacklist

Section 3(c)(8)(A)(iii) provides that nothing in Section 3(a) shall "require a covered platform operator to interoperate or share data with persons or business users that are on [a federal government blacklist]." Again, this is a welcome qualification: it is certainly better to include it than not to do so. But plenty of entities, and categories of entities, will give grounds for serious concern—including on national security grounds—without appearing on a government blacklist.

c) Foreign adversaries

Section 3(c)(8)(A)(v) provides that nothing in Section 3(a) shall be construed "in a manner that would likely result in data on the covered platform or data from another business user being transferred to the Government of the People's Republic of China or the government of a foreign adversary." This is another welcome qualification. But it is exceedingly narrow. The real danger is probably not, or not exclusively, that an entity visibly affiliated with an adversary government seeks equal treatment. The real danger is that, in practice, platforms will generally not be in a position to know whether or not an adversary government lurks behind—or has control or

influence over or access to—an entity, or a category of entities seeking access to covered platforms. And this provision seems little or no help in responding to that real-world problem.

III. THE OPEN APP MARKETS ACT (S. 2710)

I have reviewed a draft of the Open App Markets Act ("OAMA"), as reported to the Senate on February 17, 2022.[97] For the reasons explained below, I do not support OAMA in its current form. But I would support a narrower version.

A. Summary

OAMA exemplifies a much more promising approach to digital-markets regulation than AICOA. It is focused on a specific and reasonably well-defined set of markets that are similar to one another: markets for the sale and distribution of apps, and for app-store services. It is unlikely to prohibit or deter a wide array of product improvements and feature innovations. And it clearly aims to provide significant room for platforms to take reasonable measures for good reasons.

On substance, also, I generally support at least three of the bill's ideas.

First, most-favored-nation clauses ("MFNs") are commitments by a bound party to offer a beneficiary terms that are at least as favorable as those that the bound party offers to the beneficiary's competitors (or to other third parties). They can promote competition, by ensuring that the beneficiary (and its own customers) can benefit from whatever favorable terms—such as low prices—the bound party is able to provide. But they can also penalize and deter discounting that may stimulate competition with the beneficiary, because they make discounting more expensive. When used by an app store with significant market or monopoly power, I fear that MFNs clauses may do more harm than good. And I also do not much worry about the ability of large digital platforms to bargain robustly to get favorable terms.

[97] https://www.congress.gov/117/bills/s2710/BILLS-117s2710rs.pdf (OAMA Feb. 2022 draft).

Accordingly, I support a ban on app price MFNs for app stores with significant market or monopoly power. I doubt such a ban will do much harm, and I think it could do some good.

Second, I also would support a limited ban on the competitive use of competitively sensitive nonpublic business information obtained by an app store owner directly from an app developer as a condition of operating the app store. For example, I would not allow an app store owner to make competitive use of app code, business plans, or other material that it may care to demand from an app developer as a prerequisite for being allowed on the app store.

To be clear: the limited ban that I support is much narrower than OAMA's current ban on use of data. I think app stores should be free to use all other data—including data about customer demand, searches, downloads, and so on—to compete against app developers, even in its own store. I also think app store owners should be free to buy data, and developers should be free to sell it to them. Restricting app stores from doing so would be a clear case of forcing a platform to do *less* for consumers and *more* for other businesses.

Third, I would also support transparency obligations to make sure that consumers know when paid advertising is affecting a search ranking or similar placement. A mandatory disclosure like "Ad" or "Advertising" would help consumers, and harm no-one.

But I do not support the rest of OAMA, and I fear that as currently framed it would do significant harm. Above all, I fear that forcing covered companies to host third-party app stores and third-party in-app payment systems would compromise security and quality in ways that would seriously harm consumers. Cybersecurity experts have highlighted the increased dangers of third-party app stores, and the importance of careful screening of apps. I also oppose non-discrimination obligations in app carriage for the same reasons that I oppose equivalent duties in AICOA. I think

Congress should not get into the business of punishing product improvements, nor deterring platforms from protecting users.

B. Some OAMA Provisions Could Stimulate Competition and Benefit Consumers

I support narrowed versions of three of OAMA's prohibitions: a ban on app pricing MFNs for app stores with significant market or monopoly power; a ban on competitive use of competitively sensitive nonpublic business information received directly by a covered company from an app developer in the course of operating an app store, for app stores with significant market or monopoly power; and an obligation to disclose paid advertising in search rankings or other placement.

1. Banning App Pricing MFNs Could Stimulate Interplatform Competition

Although Sections 3(a)(2) and 3(a)(3) of the current draft are found under the subtitle "Exclusivity and Tying," they are more accurately described as a prohibition against "most favored nation" (or MFN) obligations focused on app pricing.

In general, an MFN obligation commits one business (the bound party) to offer another business (the beneficiary) the best terms that the bound party is offering to any third party. An MFN assures the beneficiary that it is enjoying the most favorable terms that the bound party is able to offer. It may thus improve competition by reducing negotiation costs and spreading the benefits of favorable terms such as low prices.

But an MFN may also harm competition. In particular, it may be imposed by a business with market or monopoly power as a means of making sure that its trading partners cannot induce or sponsor competition by offering more favorable terms—such as low prices—to new entrants or

existing rivals. If a trading partner tried to use favorable terms to encourage rivalry with the monopolist, the MFN obligation would ensure that those favorable terms would have to be shared with the platform monopolist itself. This would, of course, eliminate the margin of favor that could induce entry or expansion, and make the effort self-defeating. The result: less competition.

Sections 3(a)(2) and 3(a)(3) can be understood as a ban on, among other things, the use of certain app pricing MFNs by app stores. In particular, Section 3(a)(2) prohibits a covered company from "requir[ing] as a term of distribution on an app store that pricing terms or conditions of sale be equal to or more favorable on its app store than the terms or conditions under another app store." (I think there is a typo here: I think the word "under" is supposed to read "on.") With that edit, I read this rule to effectively ban a covered company from requiring that apps be supplied for the cheapest available price as a condition of carriage on the app store. Implementing the ban in Section 3(a)(2) means that businesses will be able to offer special terms (*e.g.*, promotional pricing) to other channels without being kicked off the app store as a result.

I note that the meaning of the term "conditions of sale" is unclear: it seems to reach more broadly than pricing but does not appear to include all forms of most favored treatment: I would either clarify it or remove this provision.

Section 3(a)(3) prohibits a covered company from "tak[ing] punitive action or otherwise impos[ing] less favorable terms and conditions against a developer for using or offering different pricing terms or conditions of sale through another in-app payment system or on another app store." This rule effectively bans a covered company from giving better distribution to a developer that gives the platform better terms.

I think it is fairly clear that the use of certain kinds of MFN by dominant platforms can present some of the most troubling, and least beneficial, effects associated with MFNs. There is a real risk that platforms with significant market or monopoly power may use them to suppress discounting by lower-cost alternatives. And I do not much fear that such platforms will be unable to bargain firmly for favorable prices and terms on behalf of their customers. As such, I would be supportive of an appropriately tailored ban on app pricing MFNs by app stores with significant market or monopoly power.

On the other hand, I do think covered companies should be able to truthfully inform their consumers when an app is being offered on the best available terms, for example with a little badge, icon, or text that says "best pricing online!" or similar. This will inform consumers of truthful information that matters to competition.

But accepting both of those propositions means that a line will have to be drawn somewhere in the middle, because the spectrum between them is a bit messier than one might like. In particular, Congress may wish to reflect on at least (1) whether a covered company should be able to specially place or promote apps with best-pricing status (*e.g.*, by placing them more prominently in the app store on the basis that consumers are particularly interested in such apps, or by sending promotional emails to feature some apps that are being offered at "best pricing online" prices), and (2) whether a covered company should be able to induce best-pricing status by offering other kinds of value besides preferred placement and promotion (*e.g.*, lower distribution fees).

This is a close question. My own view is that it is probably not very sensible to *both* try to ban MFNs as a condition of carriage *and* allow a covered company to buy MFN status with preferred distribution or other favorable terms. It would simply be too easy for a covered company

to provide only minimal distribution, or non-feasible distribution, to all apps except those for which an MFN pricing commitment was made, and effectively reproduce the MFN. I also do not think the sky will fall in any relevant sense if app stores are prohibited from giving or withdrawing preferential status based on the prices at which apps are available elsewhere.

Ultimately, I think consumers will be better served by preserving the opportunity for discounting through other channels to support interplatform competition than they would be served by ensuring the possibility of favored promotion for best-priced apps.

That would suggest a reasonably simple rule: a covered company may not make any benefit or value—including preferred placement or distribution—conditional on most-favored pricing status, except that a covered company may accurately inform consumers when an app is being offered at the best available price.

I would limit this rule to app stores with significant market or monopoly power. Such a determination could be made administratively (subject to judicial review) and subject to review at regular intervals or upon the petition of the covered company.

2. A Limited Data Use Ban Could Promote Competition

Section 3(c) of the current draft bans a covered company from using "nonpublic business information derived from a third-party app for the purpose of competing with that app." In its current form, as I explain below, I think this provision, coupled with the definition of "nonpublic business information" in Section 2(6), is much too broad, and would prohibit the use of data that is lawfully in the hands of the app store to better serve consumers.

There are two kinds of practice that, in my view, should be protected by any bill. First, it is important that an app store be able to use for competitive purposes the information lawfully within its own hands as a result of that role, including information about consumer demand, searches, downloads, and purchases. Just like any store that both retails and manufactures, an important source of consumer benefit is the possibility that the retail information will inform better manufacturing. That is just as true for app stores as it is for other businesses. Second, it is also important to protect the ability of an app developer to sell—and an app store to buy and use—data that can be more effectively used or commercialized by the app store owner than the developer. Preventing that sale, as Doug Melamed has pointed out, would inflict harm to no good end.[98]

But I think it would be reasonable, and perhaps beneficial, to prevent app stores from making competitive use of nonpublic, competitively sensitive information—such as app code or future business plans—received directly from an app developer as a condition of operating the store. If app store operators with market or monopoly power imposed an obligation to provide such information to the app store and could then make competitive use of it against the apps, developers' incentives to invest in valuable feature improvements would be reduced and suppressed.

In principle—and subject to closer examination (as I am not an expert on the operation of app stores!)—I think the needle can be threaded well enough by limiting the restriction to a ban on competitive use of competitively sensitive nonpublic business information (1) received directly from the developer (2) as a condition of operating the app store business, and specifically protecting the app store's right to use *all other information and data* generated by the app store or

[98] A. Douglas Melamed, *Why I Think Congress Should Not Enact the American Innovation and Choice Online Act*, Comp. Pol'y Int'l (June 19, 2022), https://www.competitionpolicyinternational.com/why-i-think-congress-should-not-enact-the-american-innovation-and-choice-online-act.

activity by anyone (customer or app developer) on or in the app store, as well as the right to enter into separate agreements for the purchase and sale of data.

In sum: I propose that a covered company should be able to make competitive use of all data, *except* competitively sensitive nonpublic business information turned over directly by the developer as a condition of access to an app store with significant market or monopoly power.[99]

3. A Requirement to Disclose Paid Advertising Through Ranking or Placement

Section 3(e) bans a covered company from engaging in certain forms of self-preferencing in app search. The provision specifically exempts "clearly disclosed advertising" in Section 3(e)(2)(B). In its current form, as I explain below, I think this provision is much too broad and will harm consumers (for reasons broadly equivalent to those discussed in the context of AICOA[100]).

But the exemption suggests a valuable rule. It would not be unreasonable to require that a covered company clearly disclose paid advertising that affects search ranking or involves preferred placement. When businesses pay for preferred app placement, consumers can easily be made aware of that fact—and disclosing advertising does not require upending algorithms or banning product improvements or procompetitive product distribution.

This could be accomplished by a specific and targeted provision requiring that any advertising for a business user involving preferred ranking, placement, or promotion be clearly disclosed, particularly by an app store with significant market or monopoly power. The FTC's

---

[99] I do appreciate that this could in principle create some opportunities for gamesmanship, by designing or operating stores in such a way as to gather additional competitively sensitive data "on" or "through" the platform rather than directly from the developer. I do not think there is a good solution to this problem that can be solved without doing more harm than good. And if forced to do so, I would probably be willing to sacrifice the benefits of the non-use rule in order to save the consumer benefits of the app store's ability to make competitive use of data.

[100] *See supra* § II.B–D.

Endorsement Guides may offer a useful framework: for example, one could imagine a provision that a covered company must "clearly and conspicuously disclose" the fact of paid promotion or preferencing.[101]

C. OAMA's Other Provisions Would Harm Consumers

I do not support the remainder of OAMA. I am particularly concerned by OAMA's forced access provisions, which I fear would threaten consumers and platforms.

1. Forcing Third Party IAPs Harms App Store Security and Viability

Section 3(a)(1) prohibits a covered company from "requir[ing] developers to use or enable an in-app payment system owned or controlled by the covered platform or any of its business partners as a condition of the distribution of an app on an app store or accessible on an operating system."

It is not quite clear what this means. Taken literally, it means that a covered company may not require that an app use the covered company's *own* IAP in order to be admitted to the app store or ecosystem, but it does not prevent a covered company from banning all other IAPs. In other words, an app store can say: "you choose—my IAP system, or no IAP system," and it will have complied with the provision. If that's the intended meaning, I don't object, but it's hard to believe that's really what anyone intends!

Nor is it really clear what "business partner" means. Suppose that an app store owner sets up an "approved IAP" program: IAP providers submit to careful checks and audits to make sure

[101] *See* FTC, Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255; *see also* FTC, The FTC's Endorsement Guides: What People Are Asking (updated Aug. 27, 2020), https://www.ftc.gov/business-guidance/resources/ftcs-endorsement-guides-what-people-are-asking.

that their IAP system is sufficiently safe and secure to be allowed on the platform. They may pay the app store for the right to be permitted in apps on the store (for this, too, is a form of distribution provided by the app store to the IAP system owner), or app developers may themselves pay for the right to use a third-party IAP. I cannot imagine why an app store should be prohibited from setting up a program of that kind.

In any event: I will assume that the intent is to re-draft the rule to require that an app store allow (some? all?) third-party IAP systems in apps sold on the store and used in the ecosystem.

Understood in this way, such a rule would generate two problems, both of which appear fairly serious. The first problem is a security one. Forcing app stores to allow third-party payment systems—or preventing or deterring them from imposing restrictions—puts consumers at risk by exposing their financial information to third parties on their platform. An app may knowingly or unknowingly choose to use an IAP that is low-quality, insecure, vulnerable to hostile or malicious actors, or simply run by those with little incentive or ability to serve consumers' interests, making it difficult for consumers to contest charges and obtain refunds.

Today, major app stores have every incentive to ensure that IAP systems are easy, secure, and safe, and that they handle requests for refunds or error corrections promptly and effectively. After all, when apps in an app store become unsafe for users, the app store becomes less appealing. Store owners also have the ability to keep consumers safe when they control the IAP. If an individual app turns out to be malicious or unsafe, a platform that controls the IAP can cut off its ability to extract funds, and can easily refund consumers.

But individual app developers do not have such an incentive. They can benefit—innocently or knowingly—from the high reputation of a platform or app store to win consumer confidence,

and expose consumers to harm after they have been downloaded and installed by an unsuspecting user. An individual app developer may choose a third-party IAP because it is cheap, because it is the first one the developer finds, or because it is part of a hostile or malicious plan.

The second problem is a commercial one. If app stores are forced to allow developers to operate their own IAP systems without a means of ensuring compensation for in-app purchases—that is, without becoming "business partners" with the IAP provider—then there is a serious threat that developers' business models will migrate overnight from charging for an app (an event on which the app store can take a commission) to charging for in-app purchases through developers' own IAPs (an event that is or may be invisible to the app store). For example, suppose that an app store charges 30% of the price of an app and all apps end up being priced at $9.99. If it then allows third party IAP systems without any means of monitoring and charging in-app payments, one would expect that overnight those apps will move to a $0.00 price point with a $9.99 in-app purchase required on first use. (Or something similar!) The result is a distortion in pricing incentives, with a sharp drop in platform revenue, and less security. App stores may in turn be forced to move to other pricing models, like flat fees, which will make many app business models entirely non-viable. (Of course: I am not suggesting that app stores should have a right to take a commission for purchases of things *other than the app itself*.)

My point is a modest one: forcing or incentivizing app stores to say "yes" to IAP providers when they would otherwise say "no" is bad for security, even while it has other benefits. And if the consequence is to allow developers to move app pricing to an invisible space, that outcome seems bad for commercial viability and likely to result in less efficient arrangements all round.

2. Forcing Off-Platform Steering Threatens App Store Viability

Section 3(b) of the current draft prohibits a covered company—anyone operating an app store or app distribution system platform with 50 million users or more in the United States—from "impos[ing] restrictions on communications of developers with the users of an app of the developer through the app or direct outreach to a use concerning legitimate business offers, such as pricing terms and product or service offerings." It allows a covered company to give a user the opportunity to consent before "collection and sharing of the data of the user by an app."

I am sympathetic to the project of this provision, and my feelings are somewhat mixed. Such a rule could have real benefits, and my first instinct was to include this in the set of rules that I would support. But on reflection I think the costs and harms would probably overwhelm the benefits. As such, I do not support the rule.

Benefits first. There is obviously plenty to be said for a rule of this kind, at least as applied to app stores with market or monopoly power. It ensures that app developers have the opportunity to provide customers with accurate information about off-platform opportunities (including promotions and differentiated offerings through other channels, such as discounted prices of which a consumer may not have been aware). It thus could promote competition with the platform itself.

But a rule of this kind presents two different risks.

The first risk seems to be an existential commercial one. There is a clear threat that app developers will use the app store to generate customer leads and will then move those customers off-platform for all paid activity, including the purchase of the app itself. This, in turn, could threaten the profitability of the app store itself, and push app stores to less efficient charging mechanisms like flat fees. (If an app store charges a flat $3 for distribution, plenty of valuable apps

would become impossible to profitably sell on the store.) From this perspective, the communication restriction can be understood as an effort to protect against developer conduct that would otherwise erode or even destroy the business case for the app store in the first place.

To make this concrete: a developer with a fully free right to communicate with users could just charge a low or zero price for the app itself and move the payment for the app off-platform ("Thanks for downloading our app for free on the Apple App Store. To use our app, you must activate it by going to [website].com, entering a code and paying $5.99."). The result would be that an app store received *zero* revenue despite conferring massive value on the app developer. That does not seem a sustainable circumstance.

The second risk is a threat to quality: specifically, the risk that the platform experience could easily be turned into a spammy and unwelcome one. Imagine if the developer of every app you had ever downloaded had the right to get your contact details from the relevant app store, and the automatic and permanent ability to contact you through emails, text messages, popup notifications, phone calls, and other forms of communication. The result would almost certainly be a barrage of marketing misery on your device: and among other things this could seriously erode the value of the app store and ecosystem. It may be instructive to imagine what would happen if all the manufacturers of products you bought at the supermarket could freely contact you in perpetuity because you bought their product. It is not clear that that would be a better world for consumers—*regardless of whether there was a one-time consent at the time of purchase*. Not every developer will respect an "unsubscribe" click, or will do so promptly.

So on balance I do not support this provision, although I will continue to try to think of a narrower version that would not threaten app store profitability or the quality of the experience.

3. The Data Non-Use Obligation Threatens Desirable Conduct

Section 3(c) bans a covered platform from using "nonpublic business information derived from a third-party app for the purpose of competing with that app."

In its current form, I think this is much too broad, and likely to be anti-consumer in its operation. In principle, as I noted above, I would not object to a prohibition on app stores making competing use of competitively sensitive nonpublic business information obtained directly from the developer as a condition of participation in the app store, rather than from the operation of the platform. If an app store owner demanded such information as a price of admission—such as the code used to perform desirable functions—incentives for apps to invest in desirable features would be stifled. But it does not seem wise to try to *ban* app stores from asking for such data, as it may well be necessary for legitimate purposes (such as security or quality audits). As such, the best solution seems to be a ban on competitive use of competitively sensitive nonpublic business information *received directly from the developer* as a condition of operating the app store.

But the current draft goes much too far. Pursuant to Section 2(6), "nonpublic business information" includes virtually all information gained in the course of operating the app store itself. Specifically, it includes: "nonpublic data that is . . . derived from a developer or an app or app store owned or controlled by a developer, including interactions between users and the app or app store of the developer; and . . . collected by a covered company in the course of operating an app store or providing an operating system."

There are two problems with this definition. First, because a covered company is itself a developer (by reason of the definition of "developer" in Section 2(4)), it appears to include

virtually all the data a covered company obtains. (This seems to be a drafting error rather than a substantive issue.)

Second, almost everything that happens on an app store is in some sense actually or arguably "derived from" the apps in the store! So this would could prohibit an app store owner from using information that consumers are, for example, interested in video-sharing apps, or that they are searching for games with a dog theme, or that they tend to be drawn to apps with a yellow icon, and responding accordingly to meet demand. It would also prevent app stores from buying—and developers from selling—valuable data that could best be commercialized by the app store owner.

Accordingly, I propose app stores should be allowed to use information gathered from the operation of the app store—including information about user and business user activity on and in the app store—for competitive purposes, and they should be allowed to buy data for competitive use from developers. Only competitively sensitive nonpublic business information received directly from the developer as a condition of participation in the app store would be protected. (On one reading of the text, this is precisely what Section 3(c) aims to capture, in which case this is just a suggestion as to drafting rather than a substantive disagreement!)

All of this assumes, of course, that it is possible in practice to live with the line of separation that I have articulated. If it is not, and if no reasonably close equivalent was available, I would probably abandon the effort to police the line and would allow full competitive use.

In addition, the broad definition of "nonpublic business information" in Section 2(6), which cuts much too broadly by including information generated by the store's own business rather than obtained directly from an app developer, should be abandoned.

4. Forcing Access for Apps and App Stores Threatens Users

Section 3(d) requires a covered company that controls both app store *and* an operating system on which that app store runs to allow users to: "choose third-party apps or app stores as defaults for [appropriate] categories"; "install third-party apps or app stores through means other than its app store"; and "hide or delete apps or app stores provided or preinstalled by the app store owner or any of its business partners."

As a threshold matter, this provision is not clearly drafted: it is not clear whether the drafter intends that a covered company can satisfy its obligation by allowing *some* third-party options, at its own election, or must allow *all* such options.

But serious harm seems likely. First, and most importantly: an obligation to allow third-party app stores would force open the gates of each operating system to the world. Operating system owners could no longer control the flow of applications and code into their own ecosystems. They would no longer be in a position to ensure the quality, compatibility, or freedom from malicious code of the apps that flow into their operating-system ecosystems, or to make sure that developers are reputable and free from hostile influence or control. This would expose consumers to serious threats: threats to quality, user privacy, financial privacy, the security of their devices (including access to cameras, microphones, and GPS location), the integrity of the operating system, and so on.

There is an overwhelming consensus among cybersecurity experts that third-party app stores, and unscreened apps, present greater danger for users and systems, serving as entry points for malware and hostile actors to obtain access to users and their data.

The **U.S. Cybersecurity and Infrastructure Security Agency** in the Department of Homeland Security says: "Reduce the risk of downloading [potentially harmful apps] by *limiting your download sources to official app stores*, such as your device's manufacturer or operating system app store. *Do not download from unknown sources*[.]"[102]

The **Federal Bureau of Investigation** "recommends only obtaining smartphone [banking] apps from *trusted sources like official app stores or directly from bank websites*."[103]

The U.S. **National Security Agency**'s Mobile Device Best Practices document states: "Install . . . only [applications] from *official application stores*."[104]

The **Federal Trade Commission** says: "Use official app stores. To reduce the risk of installing potentially harmful apps, download apps *only from official app stores*, such as your device's manufacturer or operating system app store."[105]

The **General Services Administration** says: "Allowing mobile apps to be loaded from an unknown source presents *one of the greatest risks* to GSA's environment when using mobile devices."[106]

The UK's **National Cyber Security Center**'s Threat Report on Application Stores states that "even official app stores (such as Apple's App Store and Google's Play Store) with vetting processes to detect malicious functionality in apps have been impacted by malware. Furthermore,

---

[102] https://www.cisa.gov/news-events/news/privacy-and-mobile-device-apps (emphasis added).

[103] https://www.ic3.gov/Media/Y2020/PSA200610 (emphasis added).

[104] https://media.defense.gov/2021/Sep/16/2002855921/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF (emphasis added).

[105] https://consumer.ftc.gov/articles/how-protect-your-privacy-apps (emphasis added).

[106] https://www.gsa.gov/cdnstatic/Securing_Mobile_Devices_and_Applications_%5BCIO_IT_Security_12-67_Rev_4%5D_01-26-2018.pdf, 17.

the current well-known *third party app stores* (that is, stores which are not provided by the manufacturer or the operating system provider) appear to have *less robust vetting processes, and so represent a greater risk.*"[107] It warns: "While there's [fewer] people using the most common third party app stores (compared with official app stores), a lack of robust vetting processes means that their users are *especially vulnerable to threat actors* uploading malware[.]"[108]

McAfee's 2023 Consumer Mobile Threat Report states: "*Stick to the verified stores[.]* While any app store is susceptible to hosting malicious applications, official platforms like Google Play and the Apple App Store have rigorous processes in place to both examine apps before they are released and to identify and remove malicious apps that are discovered after release. *Third-party app stores do not necessarily observe these processes, and some are even designed to intentionally distribute malware to mobile users.*"[109] And: "[I]t's essential that you download applications from official app stores like Google Play or the Apple Store."[110]

Nokia's 2021 Threat Intelligence Report contains abundant analysis of the dangers and risks. It urges: "[t]he easiest and most obvious form of prevention is to *download apps only from official app stores.*"[111] And "*[b]ecause of the risks of third-party apps, endpoint security teams have always advised users to download apps exclusively from official channels such as Google*

---

[107] UK National Cyber Security Center, Threat Report on Application Stores (2022), https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf, 7 (emphasis added).

[108] UK National Cyber Security Center, Threat Report on Application Stores (2022), https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf, 11 (emphasis added).

[109] McAfee, 2023 McAfee Consumer Mobile Threat Report, https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-mobile-threat-report-feb-2023.pdf, 8 (emphasis added).

[110] McAfee, 2023 McAfee Consumer Mobile Threat Report, https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-mobile-threat-report-feb-2023.pdf, 24.

[111] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 18 (emphasis added).

Play and the Apple App Store. But this advice is often not enough as malware writers continue to come up with new ways to get rogue apps into these official stores undetected."[112]

The 2021 Nokia report notes that the closed model of Apple's iOS has been instrumental to its security: "While Google has taken an open approach to app development and distribution, Apple has always maintained a proprietary approach, allowing downloads only through the official App Store. *As a result, Apple products have generally been considered the most secure mobile computing platform.*"[113] "Among smartphones, Android devices remain *the most targeted* by malware *due to the open environment and availability of third-party app stores.*"[114] Indeed: "Android devices make up 50.31% of all infected devices," with iOS far behind.[115]

Nokia's 2020 report urges the same point: Users should "[i]nstall *only applications that are from trusted app stores (*Google Play, Apple, Microsoft)."[116] And it repeatedly emphasizes the difference between official and third-party app stores: "Over the last few years, a significant improvement has been seen in the security of official mobile app stores. However, *third-party app stores are still rife with Trojanized applications.*"[117] "The security of official app stores, such as Google Play Store, has increased continuously. However, *the fact that Android applications can be downloaded from just about anywhere still represents a huge problem, as users are free to*

[112] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 18 (emphasis added).
[113] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 18 (emphasis added).
[114] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 8 (emphasis added).
[115] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 8 (emphasis added).
[116] Nokia Threat Intelligence Report 2020, https://onestore.nokia.com/asset/210088, 6 (emphasis added).
[117] Nokia Threat Intelligence Report 2020, https://onestore.nokia.com/asset/210088, 7 (emphasis added).

download apps from third-party app stores, where many of the applications, while functional, are Trojanized. iPhone applications . . . are for the most part limited to one source, the Apple Store."[118]

This is quite a consensus. The risks are bad enough for every user. But unsophisticated or vulnerable users—including children, seniors, and those unfamiliar with particular devices—will almost certainly not be in much of a position to protect themselves, and their infected devices will in turn present risks to others. Third-party app stores are a notorious vector for infection of devices—and devices in turn are a vector for infection of Americans' home networks. Indeed, as the 2020 Nokia report notes, "an increased number of Android malware infections has been detected in residential [*i.e.*, home] networks."[119]

There cannot be any serious room for doubt. Forcing more third-party app stores into our digital ecosystem will put consumers at greater risk.

The same is true of rules that force more third-party *apps* into app stores. It is also widely appreciated that hostile and malicious apps commonly disguise themselves as benign apps, even sneaking onto official app stores.[120] The 2021 Nokia report notes that "[s]ome types of malware are well known for masquerading as legitimate applications," and that Android malware often relies upon "[m]imicry of popular apps including health and fitness, photography, utility, personalization, and communication apps."[121] And McAfee's 2023 report explains: "[M]any malicious apps actually deliver some legitimate functionality. Just because the free photo editor or social media tracker you downloaded works, doesn't mean that it's not hiding something.

---

[118] Nokia Threat Intelligence Report 2020, https://onestore.nokia.com/asset/210088, 8 (emphasis added).

[119] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 12.

[120] *See supra* note 27 and accompanying text.

[121] Nokia Threat Intelligence Report 2021, https://onestore.nokia.com/asset/210870, 19.

Criminals often use encryption to hide their malicious code from reviewers, or they build in a delay, so the bad stuff doesn't show up until it has passed the tests. Another trick is to check the device's location and only behave badly in certain countries. Others download additional code to themselves after installation, keeping reviewers from ever seeing the malicious bits. Finally, sometimes criminals manage to infect legitimate apps by putting their code in a third-party code library that gets automatically included in the next software update."[122]

In other words: deterring app stores from restricting and supervising the flow of apps into the store will put consumers at greater risk.

Second, a general obligation to allow users to use a third-party app for *every* function on an OS—regardless of how central that function is to the OS itself—does not seem remotely plausible. Must a covered company allow a third-party file browser? A third party command line interface? A third party settings app? And so on. This provision appears to require that an operating system open itself up to third-party functions of every kind. This may not be Congress's intention.

Third, allowing consumers to delete critical apps and app stores, rather than just select others as defaults, exposes consumers to the risk that unsophisticated users—or those misled by malicious actors—will be able to degrade the functionality of their own device. It is not clear that this would be overall beneficial.

My concerns here mirror those I expressed in connection with AICOA: this amounts to a ban on closed systems, and a sharp challenge to system security, and I think that would be a mistaken and dangerous step. In particular, platforms should not face penalties for saying "no" to

[122] McAfee, 2023 McAfee Consumer Mobile Threat Report, https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-mobile-threat-report-feb-2023.pdf, 6.

third-party app stores, when such stores constitute a critical vector of threats to American consumers and families—nor for erring on the side of safety when it comes to suspicious apps.

5. A Ban on "Unreasonable" App Self-Preferencing Will Harm Consumers

Section 3(e) prohibits a covered company from "provid[ing] unequal treatment of apps in an app store through unreasonably preferencing or ranking the apps of the covered company or any of its business partners over those of other apps in organic search results." In turn, "unreasonably preferencing" is defined in Section 3(e)(2) to *include* ranking apps based on ownership by the covered company or its business partners (*i.e.*, preferring the covered company's own apps) and to *exclude* "clearly disclosed advertising." I think this is much too broad as drafted, and I expect that consumer harm would result.

First, the provision could—and I think likely would—be read to include an obligation not just to *rank* third-party apps, but to *carry* third-party apps in the first place. After all, distributing one's own apps while entirely refusing to distribute those of some, or all, third parties, is certainly a form of "preferencing." But a must-carry obligation for apps would be harmful for all the reasons that AICOA's various forced access obligations would be harmful. In short, it would expose consumers to significant increased risks, including risks to quality, privacy, security, and so on, by deterring app store owners from saying "no" in close cases. Here, as in the context of AICOA, it may be helpful to have "Russian Hacker Maps" in mind: likely rebranded "USA Trusty Maps" and owned by an intermediate holding company. By deterring app stores from saying no in a case like this one, Congress would expose consumers to an increased risk that Russian Hacker Maps would get onto Americans' phones and other devices.

Second, the provision seems to stop an app store owner from *correctly and desirably* factoring in the known benefits of its own ownership and control of individual apps. The fact that the app store owner also owns and supplies an app—and therefore is uniquely able to guarantee its quality, security, compatibility, and future behavior—is often relevant to assessing whether a consumer will want the app. Indeed, many consumers actively prefer known brands like Google, Apple, and Microsoft, and rationally value the reputation for quality and trustworthiness that these brands have obtained. Likewise, the fact that the app store owner can guarantee the quality, security, compatibility, or future behavior (including software patches and updates) of its own apps *is also* relevant to assessing whether those apps will be desirable for consumers. Ruling this out as a consideration makes no sense.

Recall that, as with self-preferencing more generally, manipulation of search results will not be in the interests of a covered platform in many cases. An app store that promotes worse own-brand apps ahead of better third-party apps will tend to drive *both* consumers and app developers to other app stores, because consumers will be less satisfied, and developers will earn less

Third, this provision will generate tremendous uncertainty and extended litigation. The concept of "unreasonable" self-preferencing remains essentially undefined, other than the two specifically treated examples. I see no alternative to endless uncertainty and abundant litigation over the extent to which self-preferencing might be "unreasonable." This process seems likely to add a ton of cost into app development and app store operation, for uncertain benefit.

6. An Equal-Access Obligation for Apps Will Harm Consumers

Section 3(f) requires a covered company to "provide access to operating system interfaces, development information, and hardware and software features to developers on a timely basis and

on terms that are equivalent or functionally equivalent to the terms for access by similar apps or functions provided by the covered company or to its business partners."

This amounts to a forced-access obligation for all third party apps to the operating system, hardware features (like cameras, microphones, and GPS locators), and software features (which could include just about anything, including software features that reflect user data or implicate privacy and security). This seems extremely unwise, for all the reasons identified in the context of AICOA's similar provisions.

It invites the two central criticisms that I make of AICOA above, and which I will therefore repeat only briefly. First, it will discourage operating system owners that also operate an app store from introducing product improvements or feature innovations for their own apps that they would be unable or unwilling to share with the whole universe of third-party app developers (including developers that may offer low quality, malicious, or unstable apps).[123]

Second, it will also deter operating system owners that also operate an app store from refusing access to apps that appear dangerous to users (or simply objectionable), but where the operating system owner is not sure that it could, or wants to, go through the hassle of proving the defense.[124] Thus, on a very important margin, it will incentivize operating system owners to protect their users less than they otherwise would. That seems dangerous and undesirable.

7. The User Security Defense is Too Narrow

Section 4(a)(1) creates an affirmative defense for conduct that is "necessary to achieve user privacy, security, or digital safety," undertaken "to prevent spam or fraud," "necessary to prevent

[123] *See supra* § II.C.1.

[124] *See supra* § II.C.2.

unlawful infringement of preexisting intellectual property," or "taken to prevent a violation of, or comply with, Federal or State law." And Section 7(b) sets the conditions for the application of the defense. It provides that, to benefit from the defense in Section 7(a), a covered company must establish by a preponderance of the evidence that it is applied consistently to apps of the covered company and other apps (*i.e.*, that the measure in question is not applied in such a way as to favor the company's own apps); is not "used as a pretext to exclude, or impose unnecessary or discriminatory terms on, third party apps, in-app payment systems, or app stores"; and is "narrowly tailored and could not be achieved through a less discriminatory and technically possible means."

Of course, it is much better to have such a provision than not to do so. But in its current form this defense is not sufficient to protect consumers for several reasons.

First, the defense omits several grounds on which an app store should probably be able to deny carriage or equal treatment. For example, it does not appear to protect a covered company that declines to give equal treatment to an app characterized by:

- objectionable content (*e.g.*, sexually explicit content, including in products, services, or apps aimed at or marketed to children; promotion of terrorism; promotion of violence or criminality);
- inaccurate, false, or outdated information;
- poor quality service;
- a threat of consumer confusion;
- a threat to the security or integrity of the platform itself (if security means "user" security, as the context and Section subtitle suggest);

- a threat to the security of other app developers (rather than users) (if security means "user" security, as the context and Section subtitle suggest);
- a threat that equal treatment would result in data, access, or interoperability being provided to the government of a foreign adversary (unless the relevant entity is specifically blacklisted or watchlisted by the federal government pursuant to Section 7(6));
- unusual technological, commercial, or other difficulties or costs of integration; or
- lack of information regarding a possible concern (*e.g.*, the ultimate ownership and control of an app, or the way in which an app will use data).

Second, it imposes an unduly restrictive "less discriminatory alternative" test. Rather than asking whether a particular practice was reasonably tailored to one of the enumerated legitimate purposes, it asks whether the measure was narrowly tailored such that it "*could not be achieved* through *less discriminatory* and *technically possible* means." (Emphasis added.) This seems to be a very onerous condition that threatens to make the defenses little or no use in many real cases. If there is *any* "technically possible" alternative that the app store "could" use—regardless of whether a rational app store would in fact use it as an alternative to the challenged practice, or even whether it would be reasonable to do so—then the defense fails and the platform is on the hook.

Third, it creates, but does not define, a "pretext" exception. If the conditions for an appropriate denial of service or carriage are present, it should not matter what the subjective thoughts of the covered company's employees might have been. To put it concretely: users should not be exposed to Russian Hacker Maps simply because, in denying it access under circumstances that create a reasonable threat to platform security or user privacy, the relevant employee had had

some subjective occurrent thoughts about competition. Like practices in like circumstances should not be treated differently because of different subjective thoughts.

Accordingly, it would be much better and simpler to provide that a measure that was in fact reasonably related to a legitimate justification would be protected conduct regardless of whatever subjective thoughts anyone had had about anything.

Of course, this provision is the critical measure that allows app stores to protect consumers. Making it too narrow will risk serious harm. And, to the extent that this affirmative defense is eroded or narrowed, app stores will face stronger incentives to just allow risky apps and actors onto the platform—and onto consumers' devices and into their homes.

8. OAMA Should Be Limited to Government Enforcement

Section 5(a)(1) provides for federal and state government enforcement. If Congress enacts a version of OAMA, I support limiting enforcement to federal and state government enforcement. (I note that the FTC enforcement provision presents the question of whether the FTC may enforce OAMA through rulemaking. Congress may wish to address this question explicitly.)

But Section 5(b) allows developers to sue covered companies for violations of OAMA, including for treble damages and attorney fees, plus prejudgment interest at the election of the court, plus injunctive relief under regular conditions.

I do not recommend empowering developers to bring or threaten treble-damages litigation under OAMA—and certainly not at first. In the hands of the federal government, an appropriately tailored version of OAMA could be enforced and applied in a manner consistent with the public interest. In the hands of all conceivable app developers—and potential *classes* of app developers

under Federal Rule of Civil Procedure 23—OAMA would be a weapon for threatening app stores with endless and expensive litigation. This would turbocharge concerns that app stores will face incentives to let close cases through the door, with the result that consumers will be exposed to more bad-quality, high-risk, or otherwise undesirable apps.

9. The National Security Exception is Too Narrow

Section 7(6) explains that nothing in OAMA should be construed to "require a covered company to interoperate or share data with persons or business users that" either "are on any list maintained by the Federal Government by which entities are identified as limited or prohibited from engaging in economic transactions as part of United States sanctions or export control regimes," or "have been identified by the Federal Government as national security, intelligence, or law enforcement risks."

I take this provision to be an effort to ensure that OAMA does not end up requiring covered app stores to carry, supply, promote, interoperate with, or otherwise support apps that pose a national security or other law enforcement threat.

But the problem is that the grounds are far too narrow. In order to benefit from this exception, a covered platform must be *knowingly dealing with an entity that has been specifically blacklisted or watchlisted by the federal government*! This is a desperately high bar that will apply to a vanishingly small number of cases.

The entities of ultimate concern here include a fairly broad array of hostile foreign governments and quasi-state actors, as well as hostile, criminal, and malicious private actors. Of equal concern are entities that may be owned, controlled, influenced by, or vulnerable to, such actors. Critically: *such ownership, control, influence, or vulnerability will not always be clear*. If

a covered company must justify any denial following lengthy and expensive litigation discharge a burden of proof, then it is less likely to deny access in the first place.

To do real work, I think this provision would need to immunize action taken by a covered platform if was reasonably related to a legitimate justification, such as protection against threats to users, businesses, the app store, or the platform. This includes malicious and hostile actors of all kinds as well as those owned, controlled, influenced by, or vulnerable to, such actors. Any action reasonably related to protection against such risks should probably be permitted. The point would be to avoid deterring covered companies from taking protective measures.

IV. A ROADMAP FOR PROMOTING COMPETITION

I understand that there is bipartisan commitment to supporting antitrust enforcement. In case it is useful to the Subcommittee, in this Part I briefly outline a four-part roadmap to doing so while avoiding the risks and concerns associated with AICOA or OAMA.[125]

A. Fully Fund Federal Enforcement

The best way to protect competition in digital markets is to ensure that digital monopolists must compete on the merits, and that unlawful transactions and practices are promptly detected and prohibited. This means, above all else, fully funding antitrust enforcement. In fact, the *most* urgent need in antitrust enforcement today—more urgent than substantive law reform, and much easier to design—is a serious infusion of resources to the agencies. The FTC Bureau of Competition and DOJ Antitrust Division have been heavily outgunned for a long time by the scale of the challenges they face.

[125] This Part draws on and incorporates material from my February 2022 testimony before the Subcommittee.

The FTC's website demonstrates the soaring workload of the agencies and the desperate imbalance between work and resources. In fiscal year 1979, there were 814 HSR filings,[126] while in fiscal year 2021 there were 3,520 HSR filings: more than four times as many.[127] But the staffing of the agency has not just failed to keep pace: shockingly, it has *declined*. In fiscal year 1979, the agency's FTE utilization was 1,746, while by fiscal year 2021, it had fallen to 1,123: a loss of more than 35%.[128] Similarly, in September 2022 testimony before this Subcommittee, AAG Jonathan Kanter indicated that "the Antitrust Division ended [fiscal year 2021] with 352 fewer employees than in 1979."[129]

In addition to the urgent need for staff, the agencies need money for experts, without whom antitrust cases against sophisticated businesses often cannot be won. For example, a recent successful hospital merger litigation—of the kind that may appear, from afar, relatively straightforward when compared to novel cases in tech markets—involved no fewer than *seven* testifying experts, with the defendants retaining five to the FTC's two.[130] (The FTC won in the trial court and prevailed on appeal.[131]) If this is the expert need for a hospital merger—a type of case in which the FTC has decades of world-leading experience and expertise—it is easy to see how enforcement targeted at novel practices in novel markets, including tech markets affecting news, urgently need serious financial backing.

---

[126] FTC, *Third Annual Report to Congress Pursuant to Section 201 of the Hart-Scott-Rodino Antitrust Improvements Act of 1976*, https://www.ftc.gov/system/files/documents/reports/3rd-report-fy-1979/3annrpt1979.pdf, 4.

[127] FTC & U.S. Dept. of Justice, *Hart-Scott-Rodino Annual Report Fiscal Year 2021*, https://www.ftc.gov/system/files/ftc_gov/pdf/p110014fy2021hsrannualreport.pdf, 2.

[128] https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation.

[129] U.S. Department of Justice, Press Release, Assistant Attorney General Jonathan Kanter of the Antitrust Division Testifies Before the Senate Judiciary Committee Hearing on Competition Policy, Antitrust, and Consumer Rights (Sept. 20, 2022), https://www.justice.gov/opa/speech/assistant-attorney-general-jonathan-kanter-antitrust-division-testifies-senate-judiciary.

[130] *FTC v. Hackensack Meridian Health, Inc.*, Case No. 20-18140, 2021 WL 4145062, at *1–2 (D.N.J. filed Aug. 4, 2021).

[131] FTC v. Hackensack Meridian Health, Inc., 30 F.4th 160, 164 (3d Cir. 2022).

The recent funding increase for DOJ and the FTC is a terrific development and a great start. The FTC's budget for fiscal year 2023 contemplates a staffing increase to 1,440 FTE and $490 million: an increase of 300 FTE and $139 million over fiscal year 2022. This is a step forward for free and competitive markets!

But it is, unfortunately, just a start. Even with the increase, FTC expected staffing will stand in 2023 at just 82.5% of fiscal year 1979 staffing[132]—and, again, recall that HSR filings are now at more than *four times* their 1979 levels! And of course the work itself is harder and more expensive than it was in 1979: today, courts are more demanding of antitrust plaintiffs; fact discovery is more burdensome and expensive than it was in 1979, including because of the vast explosion in the creation and retention of documents and data; and expensive experts are a strict necessity for antitrust litigation.[133] As the FTC's most recent budget justification notes:

> It is commonplace for defendants in FTC litigations to outspend the Commission by a significant amount on expert support, which often results in FTC experts having to conduct more extensive—and thus more costly—rebuttal analyses. In recent years, the Commission's substantial litigation docket has generated *projected expert spending that far exceeds our available budgeted resources, sometimes by as much as [five] times,* potentially threatening the Commission's ability to challenge meritorious cases.[134]

There is plenty of bang available for the taxpayer's buck here. Fully funding federal enforcement would allow the agencies to cover their docket, including, for example:

---

[132] FTC, Fiscal Year 2023 Congressional Budget Justification, https://www.ftc.gov/system/files/ftc_gov/pdf/P859900FY23CBJ.pdf, cover letter & 8.

[133] For a recent view from the litigation finance world, *see, e.g.*, Jason Levine, *The role of litigation finance in antitrust lawsuits* (Mar. 30, 2022), https://omnibridgeway.com/insights/blog/blog-posts/blog-details/global/2022/03/29/the-role-of-litigation-finance-in-antitrust-lawsuits ("The complexity and long duration of antitrust cases also make them inordinately expensive to litigate. . . . The prohibitive costs stem not only from the need for top-of-the-market counsel and expert witnesses, but also from the expense of motions practice and discovery that is comprehensive and hard-fought. Defendants frequently produce millions of documents, and the parties take dozens of depositions, even in single-plaintiff antitrust cases. This is particularly true when opt-out cases are consolidated with class actions for pretrial proceedings, as in multidistrict matters, and discovery is intermingled.").

[134] FTC, Fiscal Year 2023 Congressional Budget Justification, https://www.ftc.gov/system/files/ftc_gov/pdf/P859900FY23CBJ.pdf, 13,

- **A fuller docket of healthcare provider transactions.** Hospital and physician-practice transactions, including serial roll-up acquisitions, acquisitions of dialysis clinics, that affect both urban and rural communities and threaten Americans' access to healthcare. The FTC's elite record in hospital merger challenges—one loss since the program was rebooted roughly twenty years ago—leaves it well positioned to extend its protection over transactions outside major metropolitan areas into under-served parts of the country, including rural markets for healthcare services. This is crucial work. For example, the recent work of Thomas Wollmann highlights the dangers of "stealth consolidation"—that is, non-reportable deals—in dialysis markets across the country.[135]
- **Anticompetitive conduct in healthcare markets.** The FTC's recent action against "Pharma Bro" Martin Shkreli demonstrates the dangers of monopolizing and otherwise anticompetitive practices in healthcare markets that affect American patients and families. That case involved practices that raised the price of a critical treatment for toxoplasmosis—a parasitic infection that presents a deadly threat to immunosuppressed and immunocompromised individuals, including HIV patients and transplant recipients—by a remarkable *4,000%*, while blocking the entry of rivals that would have been able to supply American families and bring prices down. The FTC filed suit in 2020 and won at trial in 2021, resulting in a resounding FTC victory and a full remedy that included disgorgement of illegally obtained

[135] *See* Thomas Wollmann, *How to Get Away With Merger, Stealth Consolidation and its Effects on U.S. Healthcare*, NBER Working Paper 27274 (rev. July 2021), https://faculty.chicagobooth.edu/-/media/faculty/Thomas-Wollmann/Research/how_to_get_away_nber_w27274_v2.pdf.

profits and a lifetime industry ban for Shkreli.[136] This victory was obtained by the same litigating unit at the FTC that achieved the pathbreaking *Actavis* victory that exposed "pay for delay" agreements between branded incumbents and generic entrants to full antitrust scrutiny.[137] Full funding would enable this vital work to cover more markets, analyze more practices, and ultimately protect more consumers, patients, and families.

- **Transactions affecting local markets, particularly in rural and under-served locations in states where state Attorneys-General are not equipped to protect competition.** Practices and transactions affecting rural and under-served communities across the United States, including transactions that threaten competition among supermarkets, other grocery and food suppliers, gas stations, and retail banks. A merger to monopoly in a local market is still an illegal merger to monopoly! But too often such transactions are too small to justify the attention of federal enforcers with scarce resources, or over-stretched State AGs. More funding would enable the federal enforcers to show the flag in local markets and rural or under-served communities, and make it clear that there are no "small market" exceptions to the Sherman Act.
- **Transactions or practices in complex markets, such as digital and platform markets.** The agencies have been criticized in recent years for failure to challenge certain transactions in digital markets, such as Facebook's acquisition of Instagram. But the reality is that digital antitrust cases are hard to prepare, hard to litigate, and

[136] FTC v. Shkreli, 581 F. Supp. 3d 579 (S.D.N.Y. 2022).

[137] FTC v. Actavis, Inc., 570 U.S. 136 (2013).

> hard to win. Traditional metrics like market shares and nominal prices may be controversial or entirely absent; the competitive effects of particular practices may be harder to prove with confidence; and the design and application of remedies may raise tremendous complexities. And any responsible antitrust agency will (and should!) consider, when deciding how to allocate enforcement resources like staff and dollars, the risk of litigation, and the opportunity costs of the case that the agency would not be able to bring as a result. As a result, effective digital antitrust means making sure that more traditional dockets—with clearer harms in simpler markets—are covered too. When the agencies can cover the clearest and strongest cases, the case for devoting resources to more complex matters becomes stronger.

B. Support State Enforcement

State Attorneys-General play a critical role in the nation's antitrust enforcement system, but—with a handful of exceptions—seldom have the expertise, staffing, or experience to litigate a significant antitrust case alone. Accordingly, Congress may wish to consider reinforcing the antitrust enforcement capacity of the State Attorneys-General, with a contribution of funding grants and/or technical assistance. State AGs are often the first line of defense for consumers as well as critical partners to federal enforcers, but—while many offices are leading and effective voices in antitrust enforcement—others lack sufficient funding and expertise to maintain a robust antitrust enforcement program. Federal support could help to change this.

C. Modernize Antitrust Doctrine

I support the careful revision of our core antitrust statutes to ensure that markets remain free and competitive, and to clarify Congress's intention that acts and practices that harm

RESPONSES TO QUESTIONS FOR THE RECORD TO

DANIEL FRANCIS

ASSISTANT PROFESSOR OF LAW

NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE U.S. SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS

RELATING TO A HEARING ENTITLED

"REINING IN DOMINANT DIGITAL PLATFORMS: RESTORING COMPETITION TO OUR DIGITAL MARKETS"

HEARING DATE: MARCH 7, 2023

RESPONSES PREPARED: JUNE 2023

I. Senator Grassley

QUESTION: Do you believe that the Justice Department and Federal Trade Commission have the necessary expertise and resources to understand the issues, investigate allegations, and take appropriate enforcement action in the high tech area? What's your assessment of their performance so far?

RESPONSE: The staff of the Justice Department and Federal Trade Commission have considerable expertise, but they are badly under-resourced, given the scale of their work and the expense and complexity of modern antitrust litigation. My own view is that *any* antitrust system will seem unfit for purpose if it is not adequately funded and resourced. My written testimony for the March 7 hearing contains detailed discussion of the resource challenges faced by the federal enforcers. *See* Written Testimony of Daniel Francis, Hearing Entitled "Reining in Dominant Digital Platforms: Restoring Competition to Our Digital Markets" (Mar. 7, 2023) (hereinafter "Francis Written Testimony") 124–29.

Given those constraints, and the resulting need to make hard decisions about resource allocation, I think the enforcement agencies' record in antitrust enforcement in tech industries is better than critics sometimes suggest. In particular, the agencies have often brought enforcement actions—including investigations, litigations, and/or the introduction of remedies—in markets distinguished by rapid innovation, technological complexity, competitively sensitive data, network effects, and/or platform dynamics.

Of course, in some cases, federal courts have rejected the agencies' efforts to obtain relief in certain tech or tech-intensive markets. Such cases include, for example, the FTC's monopolization cases against Rambus and Qualcomm, and DOJ's efforts to block the

Sabre/Farelogix platform merger and to challenge the anti-steering rules adopted by the American Express credit-card platform.

Of course, there is plenty of room to do better. More resources, including funding for economic and technological experts and additional staff, would enable the agencies to cover their enforcement docket, even in the most complex markets.

II. Senator Tillis

QUESTION 1: What are the legitimate privacy and security concerns that could be created by the Open App Markets Act and the American Innovation and Choice Online Act? Based on these concerns, what further recommendations do you have to improve this legislation to ensure it adequately protects user privacy and security?

RESPONSE: I believe that OAMA and AICOA create serious risks of exactly this kind to users. In particular, the forced-access and equal treatment obligations that these bills create for platforms and app stores will discourage platforms from protecting users by denying access. My written testimony explains those concerns at length.

For example, as I noted in the Executive Summary of my written testimony regarding AICOA:

> Under AICOA, covered platforms will live under the dangling sword of lengthy investigations and litigations: including the threat of disruptive interim injunctive relief, which AICOA makes available on a specially lowered threshold, and the prospect that responsible executives will personally have to forfeit their compensation. As a result, platforms will be deterred from protecting consumers by denying access, preinstallation, distribution, and so on to third-party businesses, even when the platform has reasonable grounds for concern. Those grounds might

be, for example, that an app or product might be buggy or badly interoperable with the platform; low-quality; spammy; objectionable in content (e.g., sexually explicit material or the promotion of terrorism and violence); malicious; controlled or influenced by or vulnerable to a hostile power; very costly to integrate; and so on.

This deterrent effect will bite in cases where AICOA's narrow affirmative defense does not apply—it does not cover most of the grounds just described—as well as in cases where the platform could not or does not want to go fifteen rounds with the FTC to defend the decision, nor to run the risk of a massive fine and an injunction. Forcing executives to bet their own compensation when they say "no" instead of "yes" to a third party magnifies the problem.

Of course, some of those close and borderline cases will involve good actors and great products that will obtain platform access as a result of AICOA. That will certainly be a benefit. But more bad actors will still get through the door, even if the changes are made at the behest of, and in hope of helping, legitimate competitors! I do not think there is much room to doubt that AICOA will result in more bad actors and more bad products—ranging from the malicious and sinister to the merely buggy and spammy—getting access to platforms, data, consumers, devices, and ecosystems. As the Internet of Things expands and more devices go online, this means more bad actors getting easier access to consumers' lives and homes.

I think this is too high a cost. There are plenty of hostile and malicious actors in the world today searching constantly for new ways to access consumers' devices, data, and homes. And it seems a particularly bad time to make our critical digital infrastructure more vulnerable by deterring our most important platforms from protecting their own systems and users. Platform decision-makers should not be given a choice of either letting suspicious third-party apps and entities into their ecosystems or facing the threat of complaints, investigations, litigations, injunctions, and penalties (and the forfeiture of their personal compensation!).

Francis Written Testimony, 6–8; *see also id.* 37–42 (deterrence of protective conduct), 65–67 (forced access / interoperability provision).

And as I noted in the Executive Summary of my written testimony regarding OAMA:

I fear that forcing covered companies to host third party app stores and in-app payment systems would compromise security and quality in ways that would expose consumers and others to serious harms and dangers. Cybersecurity experts overwhelmingly emphasize the dangers of third party app stores and of malicious apps. It is clear that official app stores, empowered with the ability and incentive to guard against hostile code and bad actors of all kinds, are the best hope of defending consumers from a proliferating array of threats. I think it would be a terrible

> cybersecurity mistake to breach these defenses and give third party app stores, and third party apps, a new weapon to force their way into digital ecosystems.

Francis Written Testimony, 13; *see also id.* 104–06 (forcing access for apps and in-app payment systems), 111–17 (forcing access for third-party app stores).

My solution is simple: I favor eliminating the forced access, interoperability, and equal-treatment obligations from the bills.

QUESTION 2: What does the Open App Markets Act and the American Innovation and Choice Online Act do to affirmatively protect user privacy and security if platforms are required to adopt certain practices? Is this enough to prevent misuse from bad actors? Should these proposals do more to mitigate bad actors?

RESPONSE: I do not believe the existing defenses are sufficient to protect user privacy and security.

Among other things, I am concerned because the AICOA general defense includes an unduly restrictive "less discriminatory alternative" test, omits many important grounds of justification, and is too fact-intensive to give a platform much comfort. *See* Francis Written Testimony, 58–62. Because the defense is weak, I fear that AICOA will encourage platforms to harm user security and privacy, including by granting access—to data, platforms, devices, and users—to an array of third-party "bad actors." The result, I predict, will be significant user harm.

Similarly, the OAMA security defenses are too narrow and restrictive. *Id.* 119–22, 123–24. For example, as I note in my written testimony, there is no defense covering denials on the ground that an excluded app was characterized by "a threat to the security or integrity of the

platform itself (if security means "user" security, as the context and Section subtitle suggest); a threat to the security of other app developers (rather than users) (if security means "user" security, as the context and Section subtitle suggest); a threat that equal treatment would result in data, access, or interoperability being provided to the government of a foreign adversary (unless the relevant entity is specifically blacklisted or watchlisted by the federal government pursuant to Section 7(6)); [or] . . . lack of information regarding a possible concern (e.g., the ultimate ownership and control of an app, or the way in which an app will use data)." *Id.* 120–21. And "[i]f there is any "technically possible" alternative that the app store "could" use—regardless of whether a rational app store would in fact use it as an alternative to the challenged practice, or even whether it would be reasonable to do so—then the defense fails and the platform is on the hook." *Id.* 121.

And "[i]n order to benefit from [the national-security] exception, a covered platform must be knowingly dealing with an entity that has been specifically blacklisted or watchlisted by the federal government! This is a desperately high bar that will apply to a vanishingly small number of cases." *Id.* 123.

In sum, the defenses are very far from adequate, particularly in light of the broad and vague nature of the baseline obligations created by the bills.

QUESTION 3: For the Open App Markets Act and the American Innovation and Choice Online Act what is your view of the definition of the terms "covered company" and "covered platform," respectively, in these proposals? What are your thoughts about the thresholds used to define the terms "covered company" and "covered platform?"

RESPONSE: I have serious concerns that AICOA is arbitrary in scope. My written testimony explains in detail my concerns that: the "covered platform" definition appears unprincipled; a bigness criterion is unjustified (and easily evaded through divestiture!); the term "online platform" includes businesses that are neither online nor platforms; and the definition of a business user is overbroad and vague. *See* Francis Written Testimony, 81–88 (explaining concerns in detail).

Among other things, I noted that "[i]t is important to appreciate what a departure AICOA would be for U.S. competition policy. I am not aware of any other instrument of U.S. competition policy that differentiates on the basis of market capitalization or other measure of bigness. Nor am I aware of any instrument of competition policy that has so many hallmarks of an effort to pick out specific businesses for special treatment. I think that our tradition is a point of pride for our legislative and regulatory practice: we do not pick winners and losers by name, or through criteria reverse-engineered with them in mind, nor do we single out politically unsuccessful businesses for special adverse treatment. I fear that breaking that tradition could have unhappy consequences. The unpopularity of the tech targets today may not break down along partisan lines, but with a little imagination one could imagine the same device being used in the future to target big businesses that have fallen out of favor with only one party, with AICOA cited as an example. That would be unfortunate." *Id.* 83–84.

And "[a]bove all, it is not clear why the same regulatory response is appropriate for all the businesses that satisfy AICOA's thresholds and no others. For example, if the bill's concern is with durable monopoly power, why is there no requirement of durable monopoly power—or even market power—and no limitation to markets in which such power is present? Why is the raw

number of users or business users, annual sales, or market capitalization, relevant at all to the presence or absence of competitive concerns? If the concern is digital monopoly power, or digital platforms, why is the bill focused on a set of businesses that can be understood as having won the "last war," rather than others with monopoly power that may be smaller in absolute terms today but which enjoy considerable power in their respective markets? And what is the competitive concern that is common to the—very diverse—businesses that satisfy this definition, and not to other businesses? What is the basis for thinking that the competitive concerns in e-commerce markets are the same as those in search markets, or mobile operating-system markets, or app-store markets, or social networking markets, and so on?" *Id.* 84–85.

I have directionally equivalent concerns about OAMA's coverage: I do not understand why headcount measures of bigness are an appealing metric for competition-policy instruments that aim to protect consumers and user from the harms of market power.

QUESTION 4: For the Open App Markets Act and the American Innovation and Choice Online Act do the terms "covered company" and "covered platform" strike the appropriate balance of regulating entities most responsible for the respective conduct at issue? Are there any other amendments that you would make to the definition of "covered company" and "covered platform," and if so, what amendments would you make?

RESPONSE: See previous response. I will add that I think AICOA's effort to devise one set of rules for all large digital platforms is unsound in its essence. I cannot think of any reason why a desirable regulatory regime for e-commerce sites would have anything to do with a desirable

regime for internet search engines or social networks. These are radically different businesses, raising radically different competitive concerns, and we should regulate accordingly.

With respect to OAMA, I would support some targeted rules for app stores with market power. *See* Francis Written Testimony, 98–104.

QUESTION 5: Ensuring user privacy is extremely important to me, and consumers should have transparency about how their data is being used. User data is valuable in large part because it helps private businesses tailor services and goods to their customers in ways customers find helpful. Does the Open App Markets Act and the American Innovation and Choice Online Act strike the appropriate balance between ensuring consumer control of their data and permitting appropriate use of data by the platform?

RESPONSE: No. I believe AICOA and OAMA create serious privacy and security risks. See response to Question 3 above.

QUESTION 6: In your opinion is it better to consider the sort of wholesale comprehensive revisions to existing antitrust law or more targeted and precise reforms?

RESPONSE: I favor targeted, incremental improvements to existing antitrust law. I describe several possibilities in my testimony. *See* Francis Written Testimony, 129–33. I would also clarify the powers and functions of the FTC, including its power to litigate in federal court, engage in competition rulemaking, and obtain equitable monetary relief.

QUESTION 7: In your opinion does the Open App Markets Act or the American Innovation and Choice Online Act threaten to negatively impact U.S. innovation is any way? And if so, how?

RESPONSE: Yes. I fear that OAMA and AICOA threaten very serious harm to American innovation, as I explain at length in my written testimony. I specifically fear that AICOA will prohibit or deter many product improvements and feature innovations, including because a great may product improvements involve self-preferencing, and because AICOA threatens closed ecosystems and ad-supported business models. *See* Francis Written Testimony, 23–47. I also fear that OAMA will harm the commercial viability of app stores, and deter beneficial conduct by their owners and operators. *Id.* 107–10, 117–19.

QUESTION 8: NSA, NIST, DHS, FTC, and other federal agencies have raised concerns about sideloading, and recommend consumers only download apps from the store provided by the device manufacturer or operating system provider. Do you share these concerns – why or why not? How should we evaluate these proposals in light of the concerns raised by federal agencies?

RESPONSE: I do share these concerns. These concerns inform my opposition to a rule requiring forced access for third-party apps, app stores, and in-app payment systems. See Francis Written Testimony, 65–67 (AICOA), 104–06 (OAMA, in-app payment), 111–19 (OAMA, apps and app stores).

competition—and thus harm consumers and workers—are unlawful. The bills introduced by Ranking Member Lee and Chair Klobuchar represent valuable achievements and helpful contributions to this conversation.[138]

Although a full description of possible revisions and improvements is beyond the scope of this testimony, some specific recommendations include the following:

- **Section 1 Sherman Act.** The 2018 decision of the Supreme Court in *Ohio v. American Express* imposed a burden on plaintiffs to not only prove evidence of competitive harm, such as a price increase, but also to affirmatively disprove claimed offsetting benefits. In doing so it unsettled an understanding, built on decades of previous precedent, that after a plaintiff has successfully proved harm, like a price increase, the burden passes to a defendant to prove offsetting benefits. This should be corrected. The *AmEx* Court also unsettled antitrust's basic rule that a market should be defined by reference to demand-side substitutability, and the result was to procure the immediate failure of at least one DOJ enforcement action in a manner that was universally condemned (and was saved only by the action of the UK's Competition and Markets Agency). This also should be corrected.
- **Section 2 Sherman Act.** The law of Section 2 has become notoriously vague and hostile to plaintiffs: including government plaintiffs with robust economic evidence in hand. While it should be hard for a plaintiff to win a monopolization case—antitrust should not be a bailout for unsuccessful competitors—it should not be

[138] Competition and Antitrust Law Enforcement Reform Act, S.R. 225, 117th Cong. (2021); Tougher Enforcement Against Monopolists Act, S.R. 2039, 117th Cong. (2021).

virtually impossible. The erosion of monopolization law invites abuses, leaves businesses and consumers uncertain of their rights, discourages agencies from enforcing the law, undermines the credibility of the antitrust project, and fuels calls for more radical interventions that may not serve consumers. At a minimum, Congress should clarify: the legal rules applicable to claimed justifications (in particular, that as under Section 1 the existence and sufficiency of a justification under Section 2 is a matter for a defendant to prove, not for a plaintiff to disprove); the absence of any "bad purpose" requirement, given antitrust's exclusive concern with actual and likely economic effects; and—if possible—the definition of monopolization's conduct element and its relationship to lawful competition.[139]

- **Section 7 Clayton Act.** Section 7 was intended as a shield against transactions that threatened competition. It was not intended to require a plaintiff to prove to a high level of certainty, or to quantify, the specific competitive effects that would flow from a challenged merger or acquisition. Indeed, Congress specifically amended the language of the provision during legislative deliberation: striking out a requirement that the effect of a transaction "will be" substantially to lessen competition and replacing it with a requirement that the effect "may be" of this kind—*specifically* in order to provide stronger protection against dangerous deals. But the courts have lost track of Congress's intention here: forcefully restating it would help to sharpen antitrust on an important margin.

[139] For my own view, *see* Daniel Francis, *Making Sense of Monopolization*, 84 Antitrust L.J. 779 (2022).

- **Hart-Scott-Rodino Act.** The HSR Act is the foundation for merger review in the United States. It currently grants the agencies a default initial period of 30 days to review and analyze a transaction.[140] If a deal raises sufficient concerns, the agency may issue a "Second Request" for further detailed information. Once the merging parties substantially comply with that request, the agency is back on another 30-day clock. The problem is that this often leaves too short a time to review the vast amount of information included in a Second Request, to engage fully with other market participants like customers and competitors, and to analyze claimed efficiencies and possible remedies. But all of these are necessary for accurate enforcement: that is, to challenge illegal deals and to stay out of the way of those that are not illegal.

  In practice, the agencies bargain with merging parties for additional time, trading away the opportunity to receive documents or information on particular issues or from particular custodians in order to get enough time to make a sensible decision. But this is not a happy circumstance. Kneejerk timelines force agencies into premature litigate-or-leave decisions that do not promote sound enforcement, free and competitive markets, or the interests of businesses—including merging parties as well as their competitors and trading partners. Granting significant additional time after substantial compliance with a second request—changing the 30 days to, say, 90 or even 120 days—would ensure that agencies are not stuck without the time they need for a real investigation. It would also affect only a tiny fraction of

[140] *See* 15 U.S.C. § 18a.

deals, corresponding to the most competitively troubling transactions. indeed, just 1.9% of merger filings attracted a Second Request in fiscal year 2021, with the number usually hovering somewhere around 3%.[141] And, of course, only the largest deals are HSR-reportable in the first place.

I would probably pair this change with a direction to the agencies to resume the practice of Early Termination of the HSR waiting period for deals that obviously raise no competitive concerns.[142] There is no good reason to force companies to wait a month to close their deal *after* the agencies have determined that they will not investigate further: that seem to be a pure tax on mergers and should end.

D. Targeted Platform Regulation

Although I have been generally opposed to the measures under discussion, I would support careful, market-specific regulatory intervention in specific markets where competitive concerns supported such measures. These would be targeted to specific markets and to market or monopoly power tests, not bigness criteria or to specific companies. This could include:

- **Transparency and disclosure obligations in ad tech markets.** A common concern in advertising markets is that the operation of many tools and auctions is opaque to market participants, creating opportunities for manipulation, abuse, and lost competition. I would not oppose market-specific transparency and disclosure obligations (particularly for

[141] FTC & U.S. Dept. of Justice, Hart-Scott-Rodino Annual Report Fiscal Year 2021, https://www.ftc.gov/system/files/ftc_gov/pdf/p110014fy2021hsrannualreport.pdf.

[142] FTC, Press Release, FTC, DOJ Temporarily Suspend Discretionary Practice of Early Termination (Feb. 4, 2021).

entities with significant market or monopoly power) that helped publishers, advertisers, and others in the ad tech chain make informed choices among alternatives.

- **Consumer transparency obligations, especially related to advertising.** The core of some concerns about practices like search ranking manipulation is that consumers may falsely believe that they are being given a "neutral" search ranking. To the extent that this is true, and particularly for businesses with significant market or monopoly power, I would support a mandatory disclosure (*e.g.*, "Advertising") when a search ranking is in whole or part the result of paid advertising, to help consumers make informed choices. I would also not oppose a short, ordinary-language mandatory disclosure in appropriate cases to make clear that search rankings may reflect commercial interests (*e.g.*, "Search rankings may reflect a wide variety of factors, including our business interests.").
- **Market-specific ban on MFNs.** As I indicate above in my comments on OAMA, I am not opposed to a ban on the use of most-favored-nation ("MFN") clauses by entities with significant market or monopoly power *in specific markets* in which there are grounds to think that the harms of such commitments may outweigh any benefits.
- **Market-specific interoperability or portability requirements.** I am also not opposed to the introduction of certain interoperability or portability requirements *in specific markets* in which there are grounds to think that such measures would generate real benefits without unduly harming competition or users.[143] Targeting specific markets ensures that the

[143] The costs and benefits of interoperability requirements are the subject of a rich literature. In brief, they can allow smaller competitors and entrants to grow despite the presence of large incumbents; but they can also stifle incentives to invest (because benefits are shared more fully with rivals), may reduce security, and deter innovations and improvements that are incompatible with the interoperability requirements. *See, e.g.*, Herbert Hovenkamp, *Antitrust Interoperability Remedies*, Colum. L. Rev. Forum 1 (2023); Fiona Scott Morton & Michael Kades, *Interoperability as a Competition Remedy for Digital Networks*, https://ssrn.com/abstract=3808372; Comments of The American Bar Association Antitrust Law Section Regarding the American Innovation and Choice Online Act (S. 2992) Before the 117th Congress (Apr. 27, 2022), https://www.americanbar.org/content/dam/aba/administrative/antitrust_law/comments/at-comments/2022/comments-aico-act.pdf.

measure is feasible and in the interests of consumers; it also ensures that legislators and any involved agencies can plausibly formulate sensible principles and think seriously about concerns (*e.g.*, that an interoperability standard may hold up innovation or change, or soften competition rather than sharpening it). Any such requirements must provide really robust protection for security, quality, and privacy: probably in the form of a blanket rule that measures reasonably related to the protection of users, business users, or the platform are lawful.

V. CONCLUSION

In sum, although I do not support AICOA and OAMA because I fear they would do more harm than good, I would warmly welcome robust action to support vigorous antitrust enforcement, the modernization of our antitrust laws, and some targeted platform regulations. I would also be supportive of a narrower version of OAMA.

I am grateful for the opportunity to testify before the Subcommittee. I would of course be happy to assist Congress further at any time.

BEFORE THE
UNITED STATES CONGRESS

SENATE JUDICIARY COMMITTEE

SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS

"REINING IN DOMINANT DIGITAL PLATFORMS: RESTORING COMPETITION TO OUR DIGITAL MARKETS"

March 7, 2023

STATEMENT OF

AMANDA G. LEWIS

PARTNER AT THE LAW FIRM OF

CUNEO GILBERT & LADUCA, LLP

I. Introduction

Thank you, Chairwoman Klobuchar and Ranking Member Lee and full committee Chairman Durbin and full committee Ranking Member Graham for the honor of testifying before this Subcommittee on Competition Policy, Antitrust, and Consumer Rights.

A. Background

The views presented in this Statement reflect my personal views based on my experience to date as an antitrust lawyer.[1] My experience includes nearly a decade as an enforcer at the Federal Trade Commission, including the several years I spent as a counsel-detailee to the House Judiciary Committee—working on that Committee's bipartisan Digital Markets Investigation and co-authoring the Digital Markets Report.

My time in private practice has informed and strengthened my views regarding the need for legislation to address a very broken digital marketplace. From this vantage point, I have observed and advised businesses and labor as they seek to navigate the significant challenges of an economy that is increasingly dominated by just a handful of online gatekeeper platforms.

B. Bipartisan Progress Last Congress

Last Congress, we saw significant and widespread bipartisan support for antitrust reform—particularly for bills aimed at curbing the Big Tech platforms' abuse of monopoly power.

Congress's enactment of the bipartisan Merger Filing Fee Modernization Act was a significant first step toward ensuring that the agencies fighting to promote competition for the American people have the resources they need to go up against some of the biggest and most well-capitalized companies in the world. The law strengthened state enforcers by putting State Attorneys General Offices on the same footing as federal enforcers when it comes to choosing the appropriate venue to bring cases. The new law also serves to advance our national security interests by providing regulators with the information they need to thoroughly examine the influence of foreign governments in business mergers.

Both the Senate and the House Judiciary Committees held an impressive number of hearings, with testimony from a wide range of witnesses, including representatives of affected businesses, economists, experts on antitrust law, and government enforcers. In the Senate, under the leadership of Chairman Durbin, Ranking Member Grassley, Chairwoman Klobuchar, and

[1] I currently represent clients with an interest in the subject matter of this hearing. For example, I serve as outside competition policy counsel for several business coalitions including the Coalition for App Fairness and the Responsible Online Commerce Coalition, and I also serve as an antitrust advisor to the International Brotherhood of Teamsters.

Ranking Member Lee, the Judiciary Committee held several hearings that dealt with antitrust reform and digital markets.

The House Judiciary Committee also did significant work on these important issues. Under the bipartisan leadership of Chairman Nadler, Ranking Member Collins, Chairman Cicilline, and Ranking Member Sensenbrenner, the Committee conducted a 16-month Investigation of Competition in Digital Markets. As part of that investigation, the Committee examined the dominance of Amazon, Apple, Facebook, and Google, and their business practices to determine how their power affects our economy and our democracy. In addition, the Committee performed a review of existing antitrust laws, competition policies, and current enforcement levels to assess whether they should be updated and modernized to adequately address market power and anti-competitive conduct in digital markets.[2]

After this intensive and painstaking period of gathering the facts and assessing various proposed solutions, Senator Klobuchar and Senator Grassley introduced the American Innovation and Online Choice Act (AICOA) on October 18, 2021, as a companion to H.R. 3816, introduced by Representative Cicilline and Representative Buck. AICOA represents a comprehensive bill that would effectively limit the ability of large platforms to engage in anti-competitive practices such as unfairly leveraging nonpublic data or instituting discriminatory policies to disadvantage competing products. AICOA was advanced on a bipartisan basis by the House Judiciary Committee on December 21, 2022 and the Senate Judiciary Committee on March 2, 2022.

In a separate effort, Senator Blumenthal and Senator Blackburn introduced the Open App Markets Act (OAMA) on August 11, 2021, as a companion to H.R. 7030, introduced by Representative Johnson and Representative Buck. In contrast to AICOA, OAMA is a narrow bill that applies only to mobile app markets and, within those markets, targets a very specific set of harmful conduct. OAMA was advanced on a near-unanimous bipartisan basis in a markup on February 17, 2022.

Neither AICOA nor OAMA became law last Congress. After the thorough vetting of both the problems and proposed solutions that took place over the past several years, there is no need for further discussion or study. Congress should move forward with urgency to enact the American Innovation and Choice Online Act and the Open App Markets Act without further delay in order to clarify and supplement current antitrust law.

II. The Digital Marketplace is Broken.

There is global consensus that the digital marketplace is broken. Countless jurisdictions, agencies, and other entities have studied these markets and reached essentially the same conclusion: whether we are talking about the app store ecosystem, online marketplaces, social networking, general online search, or online advertising, these markets are dominated by one or

[2] I was privileged to work on this investigation as a counsel-detailee from the Federal Trade Commission and to co-author the Majority Staff Report and Recommendations.

two online gatekeeper platforms.[3] The unchecked ability of the gatekeeper platforms to abuse their monopoly power deprives consumers, other businesses, and workers[4] of the concrete benefits of competition. Following up on these studies and analyses, multiple jurisdictions have already enacted legislation or are well on their way to doing so.

If the U.S. fails to act on Big Tech in the very near future, there is no doubt that we will be relegated to rule-takers rather than rule-makers in this critical segment of the global economy. The danger of inaction poses a significant threat to the United States' role as a global leader in technology markets.

III. Congress Should Enact Legislation To Clarify and Supplement Current Antitrust Law

A. Legislation Is a More Efficient and Effective Approach to Injecting Competition into Digital Markets than Litigation.

Enforcers, as well as private plaintiffs, are engaged in lawsuits under current antitrust law to seek relief from the gatekeeper platforms' anti-competitive conduct. However, the unique challenges of digital markets plus the time and resource-intensive nature of litigation make this an inefficient, and also possibly ineffective, tool for the job. Instead, Congress can and should respond to calls for urgent action from consumer groups, the business community, and labor to pass legislation that would inject competition into digital markets.

Several circumstances make it particularly challenging for enforcers and private plaintiffs to bring and win lawsuits under existing antitrust law against the dominant platforms. First, antitrust litigation is often very costly, which disproportionately impacts the government or affected businesses bringing these suits versus companies with virtually unlimited resources.

---

[3] *See, e.g.*, U.S. Dep't of Commerce, Competition in the Mobile Application Ecosystem (Feb. 2023), https://www.ntia.gov/sites/default/files/publications/mobileappecosystemreport.pdf?_ga=2.19535932.565939331.1678125002-153658946.1675264928 [hereinafter NTIA Report]; Secretariat of the Headquarters for Digital Market Competition, Cabinet Secretariat, Competition Assessment of the Mobile Ecosystem: Interim Report Summary (Apr. 26, 2022), https://www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_22220601.pdf; Australian Competition & Consumer Commission, Digital platform services inquiry: Interim report No. 2 – App marketplaces (Mar. 2021), https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20March%202021%20interim%20report.pdf; UK Competition and Markets Authority, Online Platforms and Digital Advertising Market Study Report (July 1, 2020), https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study; UK Competition and Markets Authority, Mobile Ecosystems Market Study Report (June 10, 2022), https://www.gov.uk/cma-cases/mobile-ecosystems-market-study#final-report; Staff of Subcomm. on Antitrust, Com., & Admin. L. of the H. Comm. on the Judiciary, 116th Cong., Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations (Oct. 2020) https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf [hereinafter House Judiciary Digital Markets Report].

[4] There has not been enough attention to the impact that the dominant digital platforms' anti-competitive conduct has on workers. For example, Amazon's self-preferencing of its own logistics services places rivals such as UPS at an unfair disadvantage. The result is a race to the bottom, where workers suffer from lower-paying and lower-quality jobs.

Second, individual cases can be dragged out for over a decade before the government or plaintiff obtains any remedy from the court—which may or may not ultimately be sufficient to address the harm. Third, the platforms have an enormous information advantage and unique access to the evidence that the government or plaintiffs need to meet their burden of proof—which has been ratcheted up by the courts over time to create an extremely high bar.

Related to this last point, there is little incentive and substantial disincentive for businesses that are harmed by the gatekeeper platforms' anti-competitive conduct to share their concerns with state or federal enforcers. The threat of economic retaliation for businesses or individuals who speak out against these powerful monopolies renders them silent and with zero practical recourse to even attempt to vindicate their statutory rights under antitrust law.[5] Furthermore, this means that the crucial evidence that enforcers need to prove their cases under current law never see the light of day.

The government's ability to issue subpoenas to compel the production of evidence from third parties does not solve the problem for two primary reasons. First, if these third parties never speak up, enforcers will not know their identity or what factual information they need to request in a subpoena. Second, even if enforcers identify relevant third parties, the incentive for these third parties is to minimize the amount of information they share in order to minimize the risk of retaliation, the costs of complying with discovery requests, and burden and exposure of being required to appear as a witness at trial. For example, a small third-party seller on Amazon's marketplace could face legal bills that add up to tens of thousands of dollars if they do not want to go up against Amazon's lawyers alone and unrepresented. (The government is not permitted to provide third-party witnesses with legal advice.)

Another obstacle for access to evidence necessary to win in court is that defendants sometimes issue or threaten to issue burdensome discovery requests to third parties who have expressed concerns about the defendant company in sworn statements to the government. This appears to be an effort to gain leverage over the individual or business and extract a counter-declaration that makes them a less desirable or compelling witness.

B. Legislative Solutions

Bipartisan legislation advanced by this Committee last Congress is a more efficient and effective approach to restore competition to digital markets than litigation under existing law. The American Innovation and Choice Online Act and the Open App Markets Act are competition bills that avoid many of the pitfalls of existing antitrust law.[6] For example, AICOA's threshold of a "critical trading partner," which must be met for a platform to be covered by the

[5] *See, e.g.*, House Judiciary Digital Markets Report at 19-20.

[6] Similarly, this is a key strength of the bipartisan Competition and Transparency in Digital Advertising Act, S. 4258, which was introduced by Senator Lee, Senator Klobuchar, Senator Cruz, and Senator Blumenthal last Congress.

bill, cuts out the resource and time-intensive exercise of defining a relevant market and establishing a company's market power through the rigid calculation of market share. This is critical for digital markets, where such measures are ill-fitted to capture the extent of the dominant platforms' practical ability and incentive to abuse their gatekeeper power in ways that harm competition. With respect to OAMA, because of the consensus that the prohibited conduct is anti-competitive, unless one of the narrowly tailored affirmative defenses apply, there is no need to demonstrate market power or harm to competition.

In addition, the simple act of setting forth clear rules of the road will likely result in voluntary and affirmative compliance to a substantial degree. Two recent examples from Europe support this conclusion. Critics of the Digital Markets Act (DMA), including trade associations funded by Apple, said the sky would fall if it were passed, particularly with respect to Article 6(4) of the DMA. However, as part of its efforts to comply with the DMA, Apple is now reportedly preparing to allow third-party app stores on the iPhone.[7] Notably, Apple already allows users to download apps from alternative app stores on its desktops and laptops, instead relying on the operating system and warning and confirmation screens given to the user to protect the device and user data.[8] Apple also permits Members of Congress and some large firms to bypass Apple's App Store to install third-party apps.[9]

Similarly, in response to two investigations by the European Commission (EC) into whether Amazon abused its dominant position in e-commerce, Amazon offered a series of voluntary commitments.[10] Although critics of AICOA, including trade associations funded by Amazon, said that the passage of the bill would "break Amazon Prime," the commitments that the company voluntarily offered up in Europe overlap with several of AICOA's requirements. Regarding Prime, for example, Amazon agreed to: (i) set non-discriminatory conditions and criteria for the qualification of marketplace sellers and offers to Prime; (ii) allow Prime sellers to freely choose any carrier for their logistics and delivery services and negotiate terms directly with the carrier of their choice; and (iii) not use any information obtained through Prime about the terms and performance of third-party carriers, for its own logistics services.[11]

---

[7] Jay Peters and Mitchell Clark, *Apple is Reportedly Preparing to Allow Third-Party App Stores on the iPhone*, The Verge (Dec. 13, 2022), https://www.theverge.com/2022/12/13/23507766/apple-app-store-eu-dma-third-party-sideloading.

[8] *See*, *e.g.*, NTIA Report at 29.

[9] Leah Nylen, *Apple Says US Bill Would Make App Store Less Secure, But Its Critics Aren't So Sure*, Bloomberg (Jun. 23, 2022), https://www.bloomberg.com/news/articles/2022-06-23/apple-aapl-defends-app-store-security-from-new-us-antitrust-bill-critics#xj4y7vzkg; *see also* Apple, *Apple Developer Enterprise Program,* https://developer.apple.com/programs/enterprise/ (last visited Mar. 6, 2023).

[10] *Amazon settles two European antitrust investigations*, Responsible Online Commerce Coalition (Dec. 21, 2022), https://theroccoalition.com/amazon-settles-two-european-antitrust-investigations/

[11] European Commission Press Release IP/22/7777, Antitrust: Commission accepts commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to Buy Box and Prime (Dec. 20, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777.

IV. Conclusion

I applaud this Committee's serious and substantial efforts to study competition problems in digital markets and come up with effective bipartisan solutions, and urge Congress to swiftly pass the American Innovation and Choice Online Act and the Open App Markets Act.

Written Questions of Senator Grassley for Amanda Lewis, U.S. Senate Judiciary Committee, Antitrust Subcommittee Hearing "Reining in Dominant Digital Platforms: Restoring Competition to Our Digital Markets," March 7, 2023

Questions for Amanda Lewis

1. Do you agree with the First Amendment concerns expressed by Professor Candeub regarding the American Innovation and Online Choice Act (AIOCA)? In your opinion, does AICOA harm free speech?

ANSWER:

The American Innovation and Choice Online Act (AICOA) does not affect or jeopardize First Amendment rights. Therefore, I do not share Professor Candeub's First Amendment concerns regarding AICOA. The plain language of S. 2033 does not refer to the First Amendment or speech rights. As a pro-competition bill, AICOA will not harm free speech. To the contrary, AICOA is likely to open up competition in digital markets, resulting in increased consumer choice and additional social media avenues through which Americans can choose to exercise their right to free speech.

While I agree with Professor Candeub that AICOA would benefit from a private right of action, I do not believe AICOA's public enforcement mechanism is insufficient or a threat to free speech.

AICOA does not make it harder for a gatekeeper platform to engage in content moderation, and it does not make it easier for a gatekeeper platform to engage in content moderation. AICOA simply has nothing to do with content moderation. The American Innovation and Choice Online Act is narrowly tailored to focus solely on addressing digital platform competition issues.

Written Questions of Senator Tillis for Amanda Lewis, U.S. Senate Judiciary Committee, Antitrust Subcommittee Hearing "Reining in Dominant Digital Platforms: Restoring Competition to Our Digital Markets," March 7, 2023

Questions for Amanda Lewis

1. What are the legitimate privacy and security concerns that could be created by the Open App Markets Act and the American Innovation and Choice Online Act? Based on these concerns, what further recommendations do you have to improve this legislation to ensure it adequately protects user privacy and security?

ANSWER:

Open App Markets Act (OAMA)

The most recent version of OAMA, considered during the 117th Congress, does not create legitimate privacy and security concerns as this version adequately protects user privacy and security. For that reason, I do not have further recommendations to improve the measures from a privacy and security standpoint.

Furthermore, by opening the app store ecosystem to competition, the Open App Markets Act will likely enhance user privacy and security. A competitive marketplace will incentivize Apple and Google, as well as newcomers, to innovate and invest in enhanced user privacy and security to keep or win customers.

American Innovation and Choice Online Act (AICOA)

AICOA, as reflected in S. 2992, which was introduced in the 117th Congress, does not create legitimate privacy and security concerns as this version adequately protects user privacy and security. For that reason, I do not have further recommendations to improve the measures from a privacy and security standpoint.

Furthermore, the latest version of AICOA, S. 2033, which was introduced in June 2023, reflects additional changes that go even further to explicitly safeguard user privacy and security. To the extent there was any ambiguity about this in S. 2992, the most recent version of AICOA leaves no doubt that the bill will promote competition without compromising user privacy and security. Furthermore, AICOA will likely improve user privacy and security by restoring incentives for covered platforms such as Meta, Google, Amazon, and Apple to compete for users.

2. What does the Open App Markets Act and the American Innovation and Choice Online Act do to affirmatively protect user privacy and security if platforms are required to adopt certain practices? Is this enough to prevent misuse from bad actors? Should these proposals do more to mitigate bad actors?

ANSWER:

Open App Markets Act (OAMA)

As stated in response to Question 1, the most recent version of OAMA, considered during the 117th Congress, does not raise legitimate privacy and security concerns as this version adequately protects user privacy and security. Nothing in this bill requires a covered platform to adopt practices that would allow misuse by bad actors. In fact, OAMA explicitly provides that legitimate actions taken by a platform to protect the security and privacy of users do not violate the Act.

Furthermore, by opening the app store ecosystem to competition, the Open App Markets Act will likely enhance user privacy and security. A competitive marketplace will incentivize Apple and Google, as well as newcomers, to innovate and invest in enhanced user privacy and security to keep or win customers.

American Innovation and Choice Online Act (AICOA)

As stated in response to Question 1, AICOA, as reflected in S. 2992, which was introduced in the 117th Congress, does not create legitimate privacy and security concerns as this version adequately protects user privacy and security. Nothing in this bill requires a covered platform to adopt practices that would allow misuse by bad actors.

Furthermore, the latest version of AICOA, S. 2033, which was introduced in June 2023, reflects additional changes that go even further to explicitly safeguard user privacy and security. To the extent there was any ambiguity about this in S. 2992, the most recent version of AICOA leaves no doubt that the bill will promote competition without compromising user privacy and security.

Specifically, AICOA does not require interoperability where such access would lead to a significant cybersecurity risk. In addition, a covered platform can restrict the uninstallation of software applications or changing of default settings where they are necessary for security or to prevent data from being transferred to the Government of the People's Republic of China or the government of a foreign adversary. Finally, section 3(b) provides for a robust affirmative defense for conduct that was reasonably tailored and reasonably necessary to "protect safety, user privacy, the security of nonpublic data, or the security of the covered platform," or to prevent a violation of Federal or State law.

By opening up digital markets to competition, AICOA will likely enhance user privacy and security. A competitive marketplace will incentivize covered platforms such as Meta, Google, Amazon, and Apple, as well as newcomers, to innovate and invest in enhanced user privacy and security to keep or win customers.

3. For the Open App Markets Act and the American Innovation and Choice Online Act what is your view of the **definition of the terms "covered company" and "covered platform**," respectively, in these proposals? What are your thoughts about the thresholds used to define the terms "covered company" and "covered platform?"

ANSWER:

Open App Markets Act (OAMA)

OAMA's definition of a "covered company" is narrowly written to cover only those platforms with gatekeeper power over their respective app store ecosystems. In addition, it is reasonable to define a "covered company" as one that owns or controls an app store with over 50 million U.S. users. This definition ensures that the bill takes a tailored approach to address the most egregious ways in which Apple and Google protect and extend their parallel monopolies

over their respective app store ecosystems. To the extent that other entities that own or control an app store achieve similar gatekeeper power in the future, this definition ensures that those entities would fall within the scope of the bill.

American Innovation and Choice Online Act (AICOA)

AICOA's definition of a "covered platform" is tailored to cover only the very largest digital platforms that also possess gatekeeper power. In other words, the thresholds are purposefully set high and narrow. The definition captures only digital platforms that are of major economic significance to the U.S. economy and occupy the role of a critical trading partner for business users that effectively have now choice but to rely on the platform to reach their customers.

This definition ensures that the bill effectively targets the most egregious ways in which covered platforms such as Meta, Google, Amazon, and Apple protect and extend their monopoly power, most of which were well-documented in the House Judiciary Committee's Digital Markets Report. To the extent that other platforms achieve similar significance for the U.S. economy and a similar level of gatekeeper power in the future, this definition ensures that those entities would fall within the scope of the bill.

4. For the Open App Markets Act and the American Innovation and Choice Online Act do the terms "covered company" and "covered platform" strike the appropriate balance of regulating entities most responsible for the respective conduct at issue? Are there any other amendments that you would make to the definition of "covered company" and "covered platform," and if so, what amendments would you make?

ANSWER:

Open App Markets Act (OAMA)

As stated in response to Question 3, the term "covered company" strikes the appropriate balance of regulating entities most responsible for the respective conduct at issue. For this reason, I would not make any other amendments to the definition of this term.

American Innovation and Choice Online Act (AICOA)

As stated in response to Question 3, the term "covered platform" takes a reasonable approach to target the entities most responsible for the respective conduct at issue. In addition, this definition reflects a bipartisan compromise that was carefully constructed and well thought-out. For this reason, I would not insist on any other amendments to the definition of this term.

5. Ensuring user privacy is extremely important to me, and consumers should have transparency about how their data is being used. User data is valuable in large part because it helps private businesses tailor services and goods to their customers in ways customers find helpful. Does the Open App Markets Act and the American Innovation and Choice Online Act strike the appropriate balance between ensuring consumer control of their data and permitting appropriate use of data by the platform?

ANSWER:

Open App Markets Act (OAMA)

User privacy is also extremely important to me, and I agree that consumers should have transparency about how their data is being used. OAMA strikes the appropriate balance between ensuring consumer control of their data and permitting appropriate use of data by the platform. It is not an "either-or" proposition: by opening the app store ecosystem to competition while also including robust protections for legitimate actions to protect user security and privacy, users can benefit from competition and also be safe.

American Innovation and Choice Online Act (AICOA)

AICOA does strike the appropriate balance between ensuring consumer control of their data and permitting appropriate use of data by the platform and business users of the platform. In particular, Section 8 of the bill clearly states that no provision of AICOA may be construed "to prohibit a covered platform operator from promptly requesting and obtaining the consent of a covered platform user prior to providing access to the nonpublic, personally identifiable information of the user to a covered platform user."

While AICOA includes important interoperability requirements as a means of addressing anticompetitive conduct and lowering barriers to entry for new entrants, I also support the bipartisan Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, which was reintroduced in July 2023. The ACCESS Act would be an effective complement to AICOA, and go even further to increase market competition, encourage innovation, and increase consumer choice.

6. In your opinion is it better to consider the sort of wholesale comprehensive revisions to existing antitrust law or more targeted and precise reforms?

ANSWER:

While I support comprehensive antitrust law reform, I also support targeted and precise reforms. History shows that targeted legislation has been successful in other sectors. The Creating and Restoring Equal Access to Equivalent Samples (CREATES) Act, which became law in 2019, is just one example of this. The CREATES Act has been highly effective in addressing a subset of anticompetitive strategies that delay competition in pharmaceutical markets and increase prescription drug costs. Congress has considered several other pieces of legislation to prohibit anticompetitive practices that branded pharmaceutical companies

repeatedly employ to block patient access to lower-cost generics, and I fully support those industry-specific bills as well. These include the Stop STALLING Act (S. 148) to address citizen petition abuse, the Preserve Access to Affordable Generics and Biosimilars Act (S. 142) to address "pay-for-delay" agreements, and the Affordable Prescriptions for Patients Act of 2023 (S. 150) to address product-hopping.

Where there is clear evidence of repeated and pervasive monopolistic conduct in a specific sector with unique characteristics, as with digital markets, it is entirely appropriate to address that conduct through targeted, industry-specific legislation. That being said, comprehensive reform to our antitrust law is also necessary.

7. In your opinion does the Open App Markets Act or the American Innovation and Choice Online Act threaten to negatively impact U.S. innovation is any way? And if so, how?

ANSWER:

Open App Markets Act (OAMA)

The Open App Markets Act does not threaten to negatively impact U.S. innovation in any way. By opening the app store ecosystem to competition, OAMA will incentivize Apple and Google, as well as newcomers, to invest in new and beneficial innovation to keep or win customers.

American Innovation and Choice Online Act (AICOA)

The American Innovation and Choice Online Act does not threaten to negatively impact U.S. innovation in any way. By opening up digital markets to competition, AICOA will incentivize covered platforms such as Meta, Google, Amazon, and Apple, as well as newcomers, to invest in new and beneficial innovation to keep or win customers.

8. NSA, NIST, DHS, FTC, and other federal agencies have raised concerns about sideloading, and recommend consumers only download apps from the store provided by the device manufacturer or operating system provider. Do you share these concerns – why or why not? How should we evaluate these proposals in light of the concerns raised by federal agencies?

ANSWER:

I do not have concerns about prohibiting Apple and Google from denying users the ability to choose how they download apps on their mobile devices. According to the latest guidance from expert federal agencies and officials, legislative solutions that prohibit restrictions on sideloading, alternative app stores, and web apps would substantially benefit consumers. For example, the Department of Commerce's National Telecommunications and Information Administration (NTIA) recently stated: "While the current app store policies do offer some benefits to consumers, including the potential for tighter security controls, the [NTIA] report

found that the costs far outweigh the benefits and that privacy and security protections can still be achieved in a more competitive environment." Similarly, the Department of Justice issued a strong letter of support for the American Innovation and Choice Online Act, which reflected the entire Department's views including those of the National Security Division.

Apple's own actions demonstrate that the company can safely provide users with the option to sideload or download apps directly from a website. Apple already allows users to download apps from alternative app stores on its desktops and laptops, relying on the operating system to protect the device and user data. Apple also permits Members of Congress and some large firms to bypass Apple's App Store to install third-party apps.

As part of its efforts to comply with the Digital Markets Act (DMA) in Europe, Apple is now reportedly preparing to allow third-party app stores on the iPhone. U.S. consumers should not have less freedom than Europeans to choose how they download apps on their mobile devices.

Testimony of Chris Lewis
President and CEO, Public Knowledge

Before the
Senate Committee on the Judiciary
Subcommittee on Competition Policy, Antitrust, & Consumer Rights

Reining in Dominant Platforms: Restoring Competition to our Digital Markets

March 7, 2023

Thank you Chair Klobuchar and Ranking Member Lee for the opportunity to testify today on behalf of Public Knowledge, a nonprofit working in the public interest for over 20 years. I'm Chris Lewis, President and CEO of Public Knowledge where we fight for an open internet, free expression, and access to affordable communications tools and creative works. We see promoting robust competition online as a key part of that mission. I want to thank the Subcommittee for holding this hearing, and for all of the work you have done towards our shared goal of improving the antitrust laws and promoting competition online.

People are increasingly feeling like they have no power over – and yet are stuck with – tech giants online. Big tech companies are popular for the democratic speech they support, the ease of purchasing products, and the communities they foster. However there is a distinct downside. Consumers don't know or understand how they are being tracked and influenced. Small businesses, and often even medium and large businesses, must accept that their products will be unfairly demoted in search results, their ability to communicate with their customers limited, and their competitively sensitive business information misused, in order to access consumers through the digital platforms that dominate the internet. On social media, where so much of our modern political debate takes place, women, people of color, and other marginalized groups face harassment that pushes us out of the conversation–and radicalization pipelines have offline consequences.

I. The Problem

Surrounded by these huge and difficult problems, we have lost our collective imagination for what a better internet could look like. In advocating for consumers, we at Public Knowledge often find ourselves advocating for new innovations and new businesses that don't exist yet. Competition is one of the best ways to promote innovation. In fact, competition drives

innovation. And this is a space that desperately needs innovation to be a part of the solution to some of the scariest problems we face online.

Over the last four years, Congress has done an impressive job of researching this problem, educating Members and the public, and giving a voice to key stakeholders in hearings like this one.[1] That work was also taking place in civil society and in academia.[2] That work was also taking place in other jurisdictions across the globe.[3] Through that extensive research from so many experts, advocates, and representatives of the people, some key themes have emerged. Digital platforms form a distinct sector that need new laws and rules to address their power and protect users. Existing antitrust law will not be sufficient, yet antitrust law does have an important role to play.

Dominant digital platforms have great power in a distinct sector. These companies are embedded in so much of our lives that their power is not just economic. They control not only how we purchase products and services, but also our communications with each other, how we access news and information, and how we discuss politics and form opinions. Even consumers and

---

[1] Investigation of Competition in Digital Markets, Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary of the House of Representatives (July 2022) https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf; Senate Judiciary Committee Hearings, The Impact of Consolidation and Monopoly Power on American Innovation, Dec. 15, 2021, https://www.judiciary.senate.gov/committee-activity/hearings/the-impact-of-consolidation-and-monopoly-power-on-american-innovation; Antitrust Applied: Examining Competition in App Stores, April 21, 2021, https://www.judiciary.senate.gov/committee-activity/hearings/antitrust-applied-examining-competition-in-app-stores ; Big Data, Big Questions: Implications for Competition and Consumers, Sept. 21, 2021 https://www.judiciary.senate.gov/committee-activity/hearings/big-data-big-questions-implications-for-competition-and-consumers; Protecting Competition and Innovation in Home Technologies, June 15, 2021, https://www.judiciary.senate.gov/committee-activity/hearings/protecting-competition-and-innovation-in-home-technologies; Competition in Digital Technology Markets: Examining Acquisitions of Nascent or Potential Competitors by Digital Platforms, Sept. 24, 2019, https://www.judiciary.senate.gov/committee-activity/hearings/competition-in-digital-technology-markets-examining-acquisitions-of-nascent-or-potential-competitors-by-digital-platforms; Competition in Digital Technology Markets: Examining Self-Preferencing by Digital Platforms, March 10, 2020, https://www.judiciary.senate.gov/committee-activity/hearings/competition-in-digital-technology-markets-examining-self-preferencing-by-digital-platforms; and House Judiciary hearings https://www.congress.gov/event/116th-congress/house-event/110883.

[2] Harold Feld, The Case for the Digital Platform Act, https://www.digitalplatformact.com/; George J. Stigler Center for the Study of the Economy and the State, Committee for the Study of Digital Platforms Market Structure and Antitrust Subcommittee Report (July, 2019), https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report; Fiona Scott Morton & David Dinielli, "Roadmap for a Monopolization Case Against Google Regarding the Search Market," (June 2020), https://omidyar.com/wp-content/uploads/2020/09/Roadmap-for-a-Monopolization-Case-Against-Google-Regarding-the-Search-Market.pdf.

[3] Online Platforms and Digital Advertising Market Study, United Kingdom Competition & Markets Authority, (July 2020) https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study; Competition Policy for the Digital Era (May 2019) https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1/language-en; Digital Platforms Inquiry Final Report, Australian Competition and Consumer Commission (July 2019) https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

businesses that would prefer not to use these services find that they cannot avoid dominant platforms.[4] Their impact is so huge that inadvertent and small errors can pose serious consequences for individuals and businesses, and even for our democracy. Their level of importance has surely risen to the level where they need sector-specific laws and rules setting guardrails for their conduct.

Existing antitrust law will not be sufficient. First, because we face problems that will not be addressed by more competition alone, but second, because achieving competition in these markets is especially difficult. As with telephone communications and internet infrastructure, dominant digital platforms require additional pro-competition policy intervention for Americans to experience the benefits of dynamic competition. This requires recognizing sources of power beyond traditional market power. Dominant digital platforms often derive power from vertical integration and conglomerate integration (integration of multiple seemingly unrelated products that are neither horizontally nor vertically related), control of key bottlenecks between consumers and the products or services they seek, and from network effects. These markets tend towards tipping, making it especially difficult for antitrust enforcement and antitrust remedies to achieve lasting competition.

Antitrust has an important role to play. Especially as Congress has so far been unable to move forward with the new laws we need. We applaud the Department of Justice and Assistant Attorney General Kanter for their antitrust cases against Google, and the Federal Trade Commission and Chair Lina Khan for their antitrust case against Facebook, as well as state attorneys general who have brought similar cases. We believe these lawsuits are well-grounded in facts and law, and indicate the breadth and seriousness of the competition concerns here. The fact that these lawsuits have garnered bipartisan support of both the Biden and Trump antitrust enforcers, as well as state attorneys general of both parties, should also be a signal to Congress that this is not a partisan issue.

I want to thank this Subcommittee and Chair Klobuchar and Ranking Member Lee for ushering through the Merger Filing Fee Modernization Act last Congress to support our antitrust enforcement agencies with more funding. At Public Knowledge we look forward to working with you to make sure that this funding is appropriated and actually makes it to the FTC and DOJ so they can increase enforcement under existing law. We were also proud to have endorsed Chair Klobuchar's Competition and Antitrust Law Enforcement Reform Act (CALERA) which will help our agencies operate more efficiently and stop more anticompetitive conduct and mergers.

II. Solutions

[4] For detailed examples of this, I recommend this 2019 series from Kashmir Hill in Gizmodo. Hill, Kashmir, 2019, "I tried to Block Amazon from My Life. It Was Impossible," Gizmodo (January 22, 2019), https://gizmodo.com/i-tried-to-block-amazon-from-my-life-it-was-impossible-1830565336; "I Cut Facebook Out of My Life. Surprisingly, I Missed It," Gizmodo (January 24, 2019), https://gizmodo.com/i-cut-facebook-out-of-my-life-surprisingly-i-missed-i-1830565456; "I Cut Google Out of My Life. It Screwed Everything Up," Gizmodo (January 29, 2019), https://gizmodo.com/i-cut-google-out-of-my-life-it-screwed-up-everything-1830565500; "I Cut the 'Big 5' Tech Giants Out of My Life. It Was Hell," Gizmodo (February 7, 2019), https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

Here's the framework for how I think we can best address the variety of challenges posed by dominant digital platforms. First, the subject of this hearing: competition. We need sector-specific, pro-competition legislation to empower consumers and business users by incentivizing market entry and facilitating switching to new platforms. Second, we need transparency so that consumers and business users can make informed choices. Third, we need consumer protection laws and rules to address platform harms that won't be improved by competition. The first and most important of these would be comprehensive privacy legislation like ADPPA. Lastly, these responsibilities should be housed in a new agency: an expert digital regulator.

Competition empowers customers to choose the option that is best for them. In many markets that's the best price, but in digital platforms, where the price is often zero dollars, competition may happen along a variety of quality measures. Consumers might prefer to see fewer ads, more relevant search results, more reliable information, more customizability like filtering tools and anti-harassment tools, or even more (or less) content moderation. Business users might prefer lower prices, as well as more direct communication with their users, greater assurances that their private business data won't be used to compete against them, less lock-in and tying of platform services they don't want or need, and more options for interoperable services from a trusted third party, like fraud detection. Today, digital platforms are not accountable to the government because of a lack of regulation, or their customers because of a lack of competition. With a combination of competition and regulation, we can hold these powerful companies accountable and see better outcomes.

Competition also spurs innovation. Fighting to win or keep customers is a great incentive to find new ways to improve your products or processes. Further, a company striving to gain market share, not yet holding a strong competitive position--such as a new entrant or maverick firm--has an incentive to disrupt the status quo with big changes. It's this type of disruptive innovation that we want to see in online platforms. Is it true that ad-supported or paid content are the only two viable business models for online content? Are these content moderation fights inevitable? Does social media need to prioritize the content that makes us most angry to maximize engagement? I'd like to see what disruptive innovators might come up with to respond to these problems if given the opportunity.

Several strong bills have already garnered lots of support in Congress to promote fair competition on and against dominant digital platforms. We need new fair competition rules, like the prohibitions on self-preferencing and anticompetitive discrimination in the American Innovation and Choice Online Act (AICOA) and the Open App Markets Act (OAMA). This will make sure consumers are actually seeing the products that are best for **them**, not just the products that are best for Big Tech's bottom line. And, by taking away some of the key tools that Big Tech uses to stifle competitors and potential competitors online, fair competition rules like those found in AICOA and OAMA will also encourage new innovators to enter the market, since they'll know they can have a fair shot to actually reach consumers.

We need interoperability requirements, like those in AICOA or in the ACCESS Act, so that users can more easily leave a social media platform that isn't working for them. It often seems like no

one is happy with how social media companies are doing content moderation today, but repealing Section 230 is absolutely not the answer. It's clear that most users want content moderation, and we believe content moderation is crucial to having constructive conversations online. But there's a lot of disagreement on just what exactly that content moderation should look like. When users have a diversity of preferences, it's important to have a diversity of options available. Yet, because of a lack of interoperability, users are stuck on the platform where their friends are, instead of being able to choose based on features, like content moderation.

To actually build a better internet that works for everyone, we are going to need a new digital regulator.[5] This regulator would work together with antitrust enforcers, not in lieu of antitrust enforcement. It would have competition, privacy, and other consumer protection authorities. It could also address content moderation concerns through transparency and due process requirements, and help carefully craft the future of algorithmic oversight and accountability.

A digital regulator can improve the effectiveness of antitrust enforcement. The breakup of the Bell System is a strong example for policymakers today to learn from.[6] In that case, the Federal Communications Commission played a critical role in the breakup, helping to broaden the array of remedies the judge was able to pursue in that antitrust case. An expert regulator can be invaluable for fact-checking the claims of an antitrust target, for providing the regulatory framework on which an antitrust remedy can be based, and for shoring up an antitrust remedy where shortcomings appear.

Most importantly, it would house the expertise needed to get each of these tricky questions right. Yes, Congress has done an admirable job examining this industry and identifying problems and solutions. But this highly technical industry with complex economics is a difficult one to manage directly from Congress. Congress is responsible for addressing so many of the problems our nation faces, and they often lack the full technical expertise to examine each one in great depth and if Congress gets a detail wrong, it literally takes an act of Congress to fix it. Regulatory agencies play a critical role and can act much closer to the speed of innovation. A digital regulator can build expertise in the sector over time. It can update rules as facts on the ground change, or as new problems are revealed. Yes, Congress must give clear guidance to the regulator, but once that work is done, oversight of the agency is a much more appropriate task for Congress on an ongoing basis than trying to oversee this mammoth industry directly.

On both sides of the aisle, and on both sides of the Atlantic, there is a clear agreement that dominant digital platforms have become too powerful and must be reined in. The question remains: Can Congress meet the moment? Last Congress, there was incredible bipartisan support for platform accountability solutions like AICOA, OAMA, and ADPPA. There was so much work done to iron out the details and bring key stakeholders into the discussion. It's so

---

[5] For the best explanation of the digital platform regulator, why it's needed, and how it should be structured and operate, see Harold Feld, The Case for the Digital Platform Act (Oct. 2019) https://www.digitalplatformact.com.

[6] For an excellent detailed account of this important history and the lessons we should take from it for how to manage the power of dominant digital platforms today, see Al Kramer, "A Lesson From the Landmark AT&T Breakup: Both a Sector-specific Regulator and Antitrust Enforcers Were Needed." https://publicknowledge.org/independent-but-together-how-antitrust-and-regulation-can-work-synergistically-to-benefit-consumers/.

disappointing that we weren't able to get any of the bills focused on tech over the finish line. Republicans and Democrats have a responsibility to come to the table and find a workable solution, because the American people cannot wait any longer.

Written Questions of Senator Grassley for Chris Lewis, U.S. Senate Judiciary Committee, Antitrust Subcommittee Hearing "Reining in Dominant Digital Platforms: Restoring Competition to Our Digital Markets," March 7, 2023

Questions for Chris Lewis

How would you characterize Big Tech's practices from a consumer perspective? Can you elaborate on what you see to be consumer harms? What's the risk with these practices if they're left unchecked? In your opinion, would the American Innovation and Choice Act help address these consumer harms?

Answer:
While there have been immense benefits to consumers from many of the products that tech platforms have created, in recent years, three big concerns have become clear. The first is privacy. I'm very concerned about how Americans' data is being collected and used online. Often without their knowledge or ability to refuse, consumers face manipulation and discrimination based on inferences that companies draw based on data collected about them online. And those are just the harms if everything is going according to plan. Sometimes this sensitive data is not kept secure and can become public or fall into the wrong hands. The House has introduced bipartisan legislation, American Data Privacy Protection Act, which would greatly enhance the privacy of all people online and help curb the surveillance and profiteering practices of online platforms. We would hope the Senate would look at moving similar legislation because all people deserve to have their personal information protected.

Second, there's a lot of concern about how the platforms are moderating user generated content. Users create, have access to, and in some cases, are bombarded by a wide variety of content when they visit these platforms. This can include links to reliable news sources, or misinformation and harassment, along with the vacations, graduations, and other family updates we look forward to seeing on social media. Protecting free expression while protecting user safety and forums that foster diverse viewpoints is a difficult problem but today. Big tech companies are not doing enough to strike this balance and greater competition can support this goal.

Third, these platforms occupy a gatekeeper role where users rely on them to access other businesses. Users expect when we go to Google that we will see the search engine results that are most relevant for us. We expect that Amazon will be showing us the product that's right for us, or that the Apple App Store will show us the right app. Instead, these companies are frequently pushing users towards the result that is best for the platform and its bottom line rather than best for the user.

The American Innovation in Choice Online Act is focused on this third problem, but can also have benefits for the first two problems. While the immediate effects of gatekeeper power are seen by consumers who don't have access to a product they might want or benefit from, the long-term effects are that competitors can't get a foothold in the marketplace. As a result,

today's dominant gatekeepers can keep their powerful position without having to worry about competition.

By restoring competition to Big Tech markets, we hope to see platforms responding to user concerns instead of ignoring them. Doing so requires breaking down the unprecedented network effects that are present in social media, online marketplaces, and other digital platforms. Breaking down the power of the gatekeepers might provide some market pressure for better privacy policies, but it is not enough. As mentioned above we still need a comprehensive privacy law such as ADPPA. On the more difficult content moderation questions, increased competition might expand the diversity of options that consumers have easy access to which empowers users and preserves their power of free expression. Particularly in content moderation, users have a diversity of preferences and should have easy access to a diversity of content moderation strategies online, from the highly moderated to those that offer little to no labeling, fact checking, or other moderation.

Questions from Senator Tillis
for Chris Lewis

Witness for the Senate Committee on the Judiciary Subcommittee on Competition Policy, Antitrust, and Consumer Rights Hearing "Reining in Dominant Digital Platforms: Restoring Competition to our Digital Markets"

1. What are the legitimate privacy and security concerns that could be created by the Open App Markets Act and the American Innovation and Choice Online Act? Based on these concerns, what further recommendations do you have to improve this legislation to ensure it adequately protects user privacy and security?

Answer:
I believe the Open App Markets Act and the American Innovation and Choice Online Act take seriously their potential impact on privacy and include the necessary language to preserve the few existing privacy protections users currently have. To actually protect consumer privacy, we really need a comprehensive federal privacy law along the lines of ADPPA or stronger. We don't want consumers to have to rely on giant platform companies to protect their privacy. In the absence of privacy legislation, we don't want to leave users unprotected. We want to make sure that dominant platforms aren't able to use privacy and security as an excuse for anticompetitive conduct. Both of these pieces of legislation strike a careful balance between those two values. Unless legislators intend to directly address comprehensive privacy concerns directly with these two bills, I don't believe any additional changes are necessary to protect user privacy.

2. What does the Open App Markets Act and the American Innovation and Choice Online Act do to affirmatively protect user privacy and security if platforms are required to adopt certain practices? Is this enough to prevent misuse from bad actors? Should these proposals do more to mitigate bad actors?

Answer:
Both pieces of legislation allow platform companies some flexibility from the requirements of the law if they are acting to protect user privacy. What is really needed to prevent misuse by bad actors is a comprehensive privacy law like the ADPPA. While AICOA and OAMA are incredibly important pieces of legislation for promoting a competitive marketplace in this very important area of our economy, they are not privacy bills. Congress still needs to pass comprehensive legislation to protect all users' privacy.

3. For the Open App Markets Act and the American Innovation and Choice Online Act what is your view of the definition of the terms "covered company" and "covered platform," respectively, in these proposals? What are your thoughts about the thresholds used to define the terms "covered company" and "covered platform?"

Answer:

It can be difficult to draw the line of exactly which firms are big enough to deserve scrutiny, but in this case there is a fair degree of differentiation. We do see market capitalization as a criteria that makes clear, without a lot of gray area, which firms are so large as to distort the marketplace, and which firms do not need to be subject to these new requirements. Beyond these two bills, the creation of an expert regulator for digital platforms can serve to continue to study the innovation and development of digital platforms and inform policy makers about needed changes to definitions long into the future. In addition to passing OAMA and AICOA, we would welcome the Senate holding hearings on Senator Bennet and Welch's Digital Platform Commission Act to further investigate the long term protection of the public interest in this sector beyond competition policy.

4. For the Open App Markets Act and the American Innovation and Choice Online Act do the terms "covered company" and "covered platform" strike the appropriate balance of regulating entities most responsible for the respective conduct at issue? Are there any other amendments that you would make to the definition of "covered company" and "covered platform," and if so, what amendments would you make?

Answer:
Yes, I believe the definitions of the terms "covered company" and "covered platform" strike the right balance and I do not believe any amendments are needed. At Public Knowledge we have analyzed the benefits of non-discrimination requirements for medium-sized firms like the ones that would not fit the definition of "covered platform" in this legislation. While there can be benefits to that type of regime, it has a very different goal. A really important benefit of non-discrimination requirements for the largest firms is the impact on a smaller firm's ability to compete. The largest firms may engage in anticompetitive discrimination simply to make more money, or with a long-term goal of preventing competition and maintaining their powerful position in the marketplace. This makes anticompetitive discrimination by large firms much more pernicious than discrimination by small firms. If there is any concern about the long term sustainability of these definitions, an expert regulator of digital platforms can help study and inform policy makers on the changes in the market, however these protections under the current definitions in OAMA and AICOA are needed now.

5. Ensuring user privacy is extremely important to me, and consumers should have transparency about how their data is being used. User data is valuable in large part because it helps private businesses tailor services and goods to their customers in ways customers find helpful. Does the Open App Markets Act and the American Innovation and Choice Online Act strike the appropriate balance between ensuring consumer control of their data and permitting appropriate use of data by the platform?

Answer:
AICOA and OAMA are not privacy bills. They are designed to function well in our current marketplace where we have no federal privacy protections for users or in the future when I very much hope Congress will pass the ADPPA or something similar to grant comprehensive federal privacy protections for all users.

6. In your opinion is it better to consider the sort of wholesale comprehensive revisions to existing antitrust law or more targeted and precise reforms?

Answer:
Both comprehensive revisions to existing antitrust law and targeted reforms like the American Innovation and Choice Online Act are needed. Public Knowledge has also endorsed Senator Klobuchar's Competition and Antitrust Law Enforcement Reform Act (CALERA) as an example of the types of common sense reforms to antitrust law that should enjoy broad approval from both sides of the aisle.

7. In your opinion does the Open App Markets Act or the American Innovation and Choice Online Act threaten to negatively impact U.S. innovation is any way? And if so, how?

Answer:
No. This legislation would be a huge boon to innovation. Companies that are already in a dominant position today are often reluctant to innovate in ways that put their monopoly at risk. That's why we believe competition is often the engine of innovation. Smaller companies and start up innovators have made it clear to us that when they see that the marketplace is dominated by a few powerful firms that control who gets to compete, they are cautious to attempt to play in a market and will look elsewhere. We need this legislation to promote innovation.

8. NSA, NIST, DHS, FTC, and other federal agencies have raised concerns about sideloading, and recommend consumers only download apps from the store provided by the device manufacturer or operating system provider. Do you share these concerns – why or why not? How should we evaluate these proposals in light of the concerns raised by federal agencies?

Answer:
I'd be interested to learn more about what these agencies really said about sideloading. Unfortunately, the curation that Apple does of their App Store is already not protecting users. As reported this year in CNET and other outlets, malicious apps are frequently able to get through and cause harm, even on the App Store. On our computers, users can already download applications without the App Store vetting process. Under the Open App Markets Act, Apple could continue to offer their App Store and users could continue to choose to only download apps from that store. However users would now have a choice. There are significant barriers to entry for building a profitable app store. I don't believe it should be (or is) the position of the US government that no possible competitor can offer the same or better vetting of apps than Apple currently does. It's quite clear to me that this is an area that could benefit from competition. Apple should feel pressure to do a better job of vetting apps for the App Store. Today their App Store faces no competition among Apple customers, and therefore there is very little pressure to do so.

Testimony of Fiona Scott Morton[1]

"Reining in Dominant Digital Platforms: Restoring Competition to Our Digital Markets"

Before the Senate Committee on the Judiciary, Subcommittee on Competition Policy, Antitrust, and Consumer Rights

March 7, 2023, at 3:00 p.m.
Hart Senate Office Building, Room 216

I. Introduction

The modern interpretation and application of U.S. antitrust laws has failed to preserve competition in today's digital platform markets. While there are numerous problems with judicial interpretations of antitrust laws that deserve legislative attention,[2] there are also unique problems involving digital platforms that would require special attention even if judicial decisions in recent decades had not been so cramped. Digital platform markets suffer from a lack of new entry and expansion for a variety of reasons. Economies of scale and scope and network effects make it difficult for new entrants to reach the scale necessary to compete.[3] Large digital platforms are also in a unique position to combine their unprecedented access to user data with

---

[1] Theodore Nierenberg Professor of Economics, Yale School of Management. I thank Yale students Michael Enseki-Frank and Natalie Nogueira for their expert assistance in preparing this statement.

[2] *See* Jonathan B. Baker et al., *Joint Response to the House Judiciary Committee on the State of Antitrust Law and Implications for Protecting Competition in Digital Markets*, Wash. Ctr. Equitable Growth (Apr. 30, 2020).

[3] *See generally* Stigler Committee on Digital Platforms, *Final Report*, Stigler Center For The Study Of The Economy And The State 23-138 (2019) ("Market Structure and Antitrust Subconmittee Report," Fiona Scott Morton, Chair), https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf; Jason Furman (Reporter), et al., *Unlocking Digital Competition: Report of the Digital Competition Expert Panel* (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf; Jacques Crémer, et al., *Fairness and Contestability in the Digital Markets Act*, 40 Yale J. Regul. (forthcoming 2023).

sophisticated algorithms in order to exploit consumers and exclude competitors.[4] Barriers to entry can be especially high when platforms take advantage of the behavioral biases of consumers, or when platforms modify API's or degrade interoperability in other ways in order to handicap rivals.[5] These techniques often favor the status quo, or can be taken advantage of by the platform to make it difficult for entrants with superior offers to attract new consumers and achieve scale.[6] Incumbent digital platforms are able to exploit structural characteristics of their markets, consumer behavior, and lax antitrust enforcement to acquire, maintain, and expand their market power.

More aggressive antitrust enforcement focused on digital market abuses should have started up a decade ago, but lack of understanding of the new technologies, lack of experience in matching the resulting strategies to established jurisprudence, as well as an increasingly hostile litigation environment, discouraged action. The antitrust enforcement agencies, state attorneys general, and private litigants are now working valiantly to dislodge the monopolies that have taken root in digital platform markets. But the success of their efforts is uncertain. Under modern antitrust jurisprudence, it may be difficult for the government to prevail. Even if the cases are successful, the litigation may take years to resolve, at which point it will be difficult for the courts to fashion remedies that are effective in restoring the lost competition. Consider that the Department of Justice's case against Google alleging anticompetitive behavior in general search, which was filed in October 2020, is not scheduled to go to trial until September of 2023.[7] The government's cases generally will be tried to judges rather than juries, and so there will be additional time after trial briefing and for the judge to write an opinion, after which (we hope) there will be proceedings on remedies. And after all that, there will be appeals and possible remand of issues back to the district court.[8] Even in the most optimistic of scenarios, the harmed

---

[4] *See* Stigler, supra note 3, at 34-40; Fiona M. Scott Morton & David C. Dinielli, *Roadmap for an Antitrust Case Against Facebook*, 27 Stan. J.L. Bus. & Fin. 267 (2022); Gregory S. Crawford, et al., *Equitable Interoperability: The "Super Tool" of Digital Platform Governance*, 40 Yale J. Regul. (forthcoming 2023); Jacques Crémer, et al., *Special Advisors' Report on Competition Policy for the Digital Era*, European Commission at 2-3 (2019), https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

[5] *See, e.g.*, Susan Athey & Fiona Scott Morton, *Platform Annexation*, 84 Antitrust L.J. 677, 81 (2022) (observing that a dominant platform can cement its market power by reducing interoperability in ways that interfere with multihoming that might otherwise benefit rivals); https://siepr.stanford.edu/publications/working-paper/platform-annexation.

[6] *See* Stigler Comm. on Digit. Platforms, *supra* note 3.

[7] *See* Lauren Feiner, *DOJ case against Google likely won't go to trial until late 2023, judge says*, CNBC (Dec. 12, 2020), https://www.cnbc.com/2020/12/18/doj-case-against-google-likely-wont-go-to-trial-until-late-2023-judge-says.html.

[8] Data in 2019 indicated the median time interval in the U.S. Court of Appeals for the District of Columbia Circuit was almost ten months. *See* https://www.uscourts.gov/sites/default/files/data_tables/. We can assume that appeals from complex antitrust matters such as these may take far longer to resolve than the ten-month median.

consumers are unlikely to experience competition in these platform markets for many years after investigations are opened and complaints filed.

In addition, there is the vexing problem of how to restore competition in the face of entrenched market power and many years of technological change deployed by the platform for its own benefit. In the absence of prompt and effective remedies that create competition in platform markets, a good alternative is a set of rules that stimulates competition *on* a dominant platform. For example, until there is entry of additional mobile operating systems that offer developers choice, neither of the two vertically integrated app stores available to US consumers has much reason to compete for developers on price or quality. However, when regulation requires that rival app stores have equal access to the mobile OS platform, then a developer can choose to distribute its app through a rival store with a more favorable curation policy, installed base, or fee level. Competition *on* the platform will benefit developers, and through lower prices and more innovation, will benefit end consumers as well.

I understand that this hearing will focus on two bills this committee advanced in the prior Congress: the American Innovation and Choice Online Act (AICOA), and the Open App Markets Act (OAMA). Both bills made it out of committee last year and so I will not provide a detailed analysis of their provisions. But, taking them as a whole, I am convinced the two bills give enforcers many of the tools they need to effectively and promptly increase competition to digital markets. These bills control the damaging behavior of dominant digital platforms by opening up markets and allowing for entry and innovation. The American Innovation and Choice Online Act forbids harmful self-preferencing, anti-competitive contractual limitations, abuse of data, impeding interoperability, and unfair discrimination in search and rankings. By limiting that conduct, the law can be expected to create opportunities for entry and expansion, new innovations and lower prices for consumers. Similarly, by allowing competition for app store payment and curation options, the Open App Markets Act will open the door for app store competition and innovation.

II. Concerns About the Bills and Their Potential Negative Consequences Are Overblown

I have read a number of opinion pieces expressing concern about the significance of the behavioral changes these bills mandate. Many of the critiques seem to presume that laws that require significant changes are bound to generate a set of equally significant negative consequences, both predicted and unforeseen. I believe this is an over-reaction.[9] The bills are carefully crafted to target a narrow range of activity while at the same time containing significant

[9] This observation served as motivation for me to join with two co-authors to write a letter in support of AICOA, which we also published publicly. *See* Fiona M. Scott Morton et al., *Why Congress Should Pass The American Innovation and Choice Online Act*, ProMarket (July 8, 2022), https://www.promarket.org/2022/07/08/why-congress-should-pass-the-american-innovation-and-choice-online-act/.

protections for platforms. Any new enforcement will occur within existing conceptual and legal frameworks which militate against extreme outcomes.

For example, AICOA is at heart a competition policy bill; it aims to restore competition to digital markets that are concentrated or monopolized. The bill is fit to its purpose, and makes actionable only those violations that *injure competition*. For some prohibitions enforcers must prove harm to competition, and for others the platforms can defend by showing their conduct *has not* harmed competition. Companies that will be subject to the prohibitions are large and sophisticated. They understand what sorts of behaviors might injure competition and which sorts would not. They therefore will make the investments necessary to avoid actions that could harm competition (this is what we want platforms to do) but are unlikely to eliminate popular products or features simply due to the risk of misinterpretation of the law.

Another concern commonly voiced is that some prohibitions will expose user data to hacking or force platforms to change their architecture in ways that make them more vulnerable to hostile foreign interests. AICOA has a built-in safeguard against this sort of risk in the form of an affirmative defense: conduct that violates one of the prohibitions nonetheless cannot support liability if it was reasonably necessary to protect user privacy, data or platform security, or, importantly, user safety.

I am not a lawyer. However, I have worked with lawyers to develop cases and then advised them as the cases proceed, most notably when I served as chief economist in the Antitrust Division. I have also served as a testifying witness, including in matters where plaintiffs have shown harm to competition and those where defendants have demonstrated affirmative defenses. These experiences bolster my confidence that the harm to competition requirements will screen out actions that are not likely to benefit competition or consumers. The deference generally given to affirmative defenses in our current system indicates that the law is very unlikely to penalize reasonable actions platforms take to protect themselves and their users. By achieving this balance, AICOA ensures that platforms as well as businesses dependent on platforms have a full opportunity to flourish and meet consumers' needs.

Another concern is that the language of the prohibition is new, or varies slightly from language used to describe similar concepts in other laws. This is a feature, not a bug. The whole idea is to set up new rules for platforms that will generate more competition. If there was nothing new in the law, it would not be doing its job. Novelty will generate some uncertainty, but this is inevitable if the goal is change. Moreover, the bill has provisions that directly address this concern as well. AICOA requires that the Department of Justice and the FTC work together to generate, develop, and issue joint enforcement guidance. Because the process for developing the guidance will include an opportunity for public comment, firms with concerns about the clarity of particular provisions can help bring about the needed clarity by explaining the ambiguities and

suggesting solutions. Moreover, each agency will bring to the process its own experience, perspective, and expertise. Importantly, by requiring that the DOJ and FTC jointly develop enforcement guidance, any legitimate concerns about how the balancing of factors called for in this legislation will reflect the statutory goals will be worked out by officials who already have the duty to protect security, privacy, and consumers alongside their antitrust enforcement roles.[10]

I am one of many academics, advocates, and policy makers who contend that a specialist regulator, instructed by Congress to issue guidelines that implement specific goals, would be a more effective and lower cost solution to regulating digital platforms. Such a regulator could respond more quickly than courts and be more nimble in responding to new technologies. Such a regulator could employ or consult with technological specialists and take into account issues such as national security, safety, and privacy, as well as competition. Senators Bennet and Welch have proposed legislation that would create such an agency.[11] Their proposal is an excellent starting point and should be seriously considered. I expect it will take many years until we have a digital regulator, just as it took much human suffering before Congress chose to create regulators for industries like pharmaceuticals and railroads. Until we have such a regulator, the laws being proposed today are the best route to immediate improvements in the welfare of consumers.

III. The Global Context of Digital Regulation Demonstrates the Urgent Need for These Laws

The pair of bills we are discussing today come at a time when the rest of the world is already moving ahead on reforming competition law in digital markets. The European Union has already passed the Digital Markets Act regulating the conduct of digital gatekeepers. The British Parliament has also announced its intention to create a Digital Markets Unit, housed within the British competition authority, which will be endowed with broad powers to regulate digital markets.

A description of the duties and obligations imposed by the European Digital Markets Act illustrates how the largest tech platforms are already obligated to adjust their business practices across Europe - with compliance required by January 2024 - to meet many of the requirements proposed in the legislation under discussion today. Below I provide a partial list, including

---

[10] The Department of Justice maintains a Computer Crime and Intellectual Property Section within the Criminal Division, which in turn houses a Cybersecurity Unit. *See* https://www.justice.gov/criminal-ccips/cybersecurity-unit. The Office of Justice Programs maintains a special feature on Internet Safety. *See* https://www.ojp.gov/feature/internet-safety/general-information. All specialized components of the Department, including the Antitrust Division, report to the Attorney General who harmonizes input from across the Department in response to legislative mandates.

[11] *See* Digital Platform Commission Act of 2022, S. 4201, 117th Cong. (2022) (proposing a new federal regulator of digital platforms).

highly abbreviated text, of the rules in Articles 5 and 6 of the DMA to illustrate similarities with the content in the bills under discussion today:[12]

Article 5(2) — Prohibition of the combining of data across core platform services.

> "The gatekeeper shall not do any of the following:
>
> …combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services"

Article 5(3) — Prohibition of wide and narrow most-favored nation clauses.

> "The gatekeeper shall not prevent business users from offering the same products or services to end users through third-party online intermediation services or through their own direct online sales channel at prices or conditions that are different from those offered through the online intermediation services of the gatekeeper."

Article 5(4) — Anti-steering and anti-gag rule allowing business users to disintermediate the platform .

> "The gatekeeper shall allow business users, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels, and to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the gatekeeper."

Article 5(5) — "reader app" rule allowing business users to disintermediate the platform.

> "The gatekeeper shall allow end users to access and use, through its core platform services, content, subscriptions, features or other items, by using the software application of a business user, including where those end users acquired such items from the relevant business user without using the core platform services of the gatekeeper."

[12] Interested readers can find the complete English language text of the DMA here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC. A "print friendly" PDF of the English language text can be found here: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423.

Article 5(7) — Prohibition on tying a platform with in-app purchase payment systems.

"The gatekeeper shall not require end users to use, or business users to use, to offer, or to interoperate with, an identification service, a web browser engine or a payment service, or technical services that support the provision of payment services, such as payment systems for in-app purchases, of that gatekeeper in the context of services provided by the business users using that gatekeeper's core platform services."

Article 5(8) — Prohibition on tying.

"The gatekeeper shall not require business users or end users to subscribe to, or register with, any further core platform services… as a condition for being able to use, access, sign up for or registering with any of that gatekeeper's core platform services…"

Article 5(9) — Transparency for advertisers.

"The gatekeeper shall provide each advertiser to which it supplies online advertising services, or third parties authorised by advertisers, upon the advertiser's request, with information on a daily basis free of charge, concerning each advertisement placed by the advertiser, regarding:

(a) the price and fees paid by that advertiser, including any deductions and surcharges, for each of the relevant online advertising services provided by the gatekeeper,
(b) the remuneration received by the publisher, including any deductions and surcharges, subject to the publisher's consent; and
(c) the metrics on which each of the prices, fees and remunerations are calculated.

Article 5(10) — Transparency for publishers.

"The gatekeeper shall provide each publisher to which it supplies online advertising services, or third parties authorised by publishers, upon the publisher's request, with free of charge information on a daily basis, concerning each advertisement displayed on the publisher's inventory, regarding:

(a) the remuneration received and the fees paid by that publisher, including any deductions and surcharges, for each of the relevant online advertising services provided by the gatekeeper;
(b) the price paid by the advertiser, including any deductions and surcharges, subject to the advertiser's consent; and
(c) the metrics on which each of the prices and remunerations are calculated.

Article 6(2) — Prohibition of use of non-public business user data to compete against the business users.

> "The gatekeeper shall not use, in competition with business users, any data that is not publicly available that is generated or provided by those business users in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services, including data generated or provided by the customers of those business users."

Article 6(3) — Obligation to offer right to un-install software and make choices over defaults.

> "The gatekeeper shall allow and technically enable end users to easily un-install any software applications on the operating system of the gatekeeper, … The gatekeeper shall allow and technically enable end users to easily change default settings on the operating system, virtual assistant and web browser of the gatekeeper that direct or steer end users to products or services provided by the gatekeeper."

Article 6(4) — Obligation to open operating systems to third–party apps and app stores.

> "The gatekeeper shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper."

Article 6(5) — Prohibition of self-preferencing in indexing and ranking.

> "The gatekeeper shall not treat more favourably, in ranking and related indexing and crawling, services and products offered by the gatekeeper itself than similar services or products of a third party. The gatekeeper shall apply transparent, fair and non-discriminatory conditions to such ranking."

Article 6(6) — Prohibition of blocking switching among apps and services accessed on the platform.

> "The gatekeeper shall not restrict technically or otherwise the ability of end users to switch between, and subscribe to, different software applications and services that are accessed using the core platform services of the gatekeeper…"

Article 6(7) — Free interoperability for business users equivalent to that enjoyed by the platform's own hardware or software.

> "The gatekeeper shall allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system or virtual assistant … as are available to services or hardware provided by the gatekeeper."

Article 6(8) — Obligation to provide tools to measure ad verification for publishers and advertisers.

> "The gatekeeper shall provide advertisers and publishers, as well as third parties authorised by advertisers and publishers, upon their request and free of charge, with access to the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements inventory, including aggregated and non-aggregated data. Such data shall be provided in a manner that enables advertisers and publishers to run their own verification and measurement tools to assess the performance of the core platform services provided for by the gatekeepers."

Article 6(9) — Obligation to enable free, real-time, end user data portability.

> "The gatekeeper shall provide end users and third parties authorised by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, tools to facilitate the effective exercise of such data portability, and including by the provision of continuous and real-time access to such data."

Article 6(10) — Obligation to grant business users access to data resulting from their activity on the platform.

> "The gatekeeper shall provide business users and third parties authorised by a business user, at their request, free of charge, with effective, high-quality, continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of the use of the relevant core platform services or services provided together with, or in support of, the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users."

Article 6(11) — Obligation to grant competitors FRAND access to online search data.

> "The gatekeeper shall provide to any third-party undertaking providing online search engines, at its request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines. Any such query, click and view data that constitutes personal data shall be anonymised."

Article 6(12) — Obligation for app stores, search engines and social networks to apply FRAND access conditions for business users.

> "The gatekeeper shall apply fair, reasonable, and non-discriminatory general conditions of access for business users to its software application stores, online search engines and online social networking services listed in the designation decision pursuant to Article 3(9)."

This list of DMA requirements demonstrates that the DMA prohibits many of the anti-competitive practices addressed in the US bills we are discussing today (perhaps because they are trying to fix the same problems). The DMA is more detailed than the text of AICOA and OAMA, and does not include any efficiency defense. Note particularly, that DMA does not require that the regulator show that each instance of prohibited conduct harms competition. Instead, the rules were chosen to be those that, in the view of the European Parliament, would generally protect and increase competition.

What does this mean for the bills we are discussing today? Unless Congress passes some form of sensible regulation, companies that seek to compete against today's dominant platforms, or offer services through them, will have an enormous incentive to focus their efforts in Europe, bringing new services, innovations and lower prices to European consumers. The most dominant tech giants will adjust their business models and practices to benefit small businesses and consumers in Europe. American businesses and consumers will be able to read about these innovations, but they will need to launch a product in Europe, or go on vacation there, to experience them. The United States will miss out on opportunities to lead the world in tech sector innovation and experience the benefits it delivers.

The UK is in the process of catching up with Europe through legislation that will allow the UK's Competition and Markets Authority ("CMA") to design platform-specific rules. These rules have the goals of both protecting consumers and increasing competition.[13] The CMA has

[13] CHANCELLOR OF THE EXCHEQUER, AUTUMN STATEMENT 2022 CP 751 35 (2022) ("The government will bring forward the Digital Markets, Competition and Consumer Bill . . . to provide the Competition and Markets Authority with new powers to promote and tackle anti-competitive practice in digital markets."), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/111841

already built the team to analyze platform conduct and design such rules, and has carried out several of the initial studies required. The expectation is that regulation in the UK will not long lag that of the EU.[14] As noted above, the DMA takes effect in January 2024 which is only nine months away. Given these substantial changes in Europe and the likely business responses to them, it is important for the US to move quickly to avoid losing the edge in innovation, and ceding the terms for digital market regulation and competition to other nations.

Dated: March 6, 2023

/s/

Fiona Scott Morton
New Haven, Connecticut

7/CCS1022065440-001_SECURE_HMT_Autumn_Statement_November_2022_Web_accessible__1_.pdf

[14] *See generally Digital Markets Unit,* Gov.UK, https://www.gov.uk/government/collections/digital-markets-unit; *see also* Her Majesty Queen Elizabeth, *Queen's Speech 2022: Her Majesty's most gracious speech to both Houses of Parliament* (May 10, 2022) ("Draft legislation to promote competition, strengthen consumer rights and protect households and businesses will be published. Measures will also be published to create new competition rules for digital markets and the largest digital firms [Draft Digital Markets, Competition and Consumer Bill] . . . ."), https://www.gov.uk/government/speeches/queens-speech-2022,

Written Questions of Senator Grassley for Fiona Morton, U.S. Senate Judiciary Committee, Antitrust Subcommittee Hearing "Reining in Dominant Digital Platforms: Restoring Competition to Our Digital Markets," March 7, 2023

Questions for Fiona Morton

Do you believe that the Justice Department and Federal Trade Commission have the necessary expertise and resources to understand the issues, investigate allegations, and take appropriate enforcement action in the high tech area? What's your assessment of their performance so far?

Answer

While I believe that the antitrust enforcement agencies have the skills it takes to enforce the law effectively in the high tech area, I also believe digital markets have unique attributes which require Congress to update the antitrust laws and provider broader regulation in order to open digital markets to robust competition and innovation. Existing jurisprudence places too many hurdles in the path of an agency attempting to combat anticompetitive behavior. The Department and FTC were slow to challenge anticompetitive behavior in these markets, but have picked up the pace recently. However, without broader enforcement tools and new regulatory authority, current antitrust efforts will not be enough to open key digital markets to new entry and meaningful paths to grow competition and innovation.

Questions from Senator Tillis
for Fiona Scott Morton
Witness for the Senate Committee on the Judiciary Subcommittee on Competition Policy, Antitrust, and Consumer Rights Hearing "Reining in Dominant Digital Platforms: Restoring Competition to our Digital Markets"

1. What are the legitimate privacy and security concerns that could be created by the Open App Markets Act and the American Innovation and Choice Online Act? Based on these concerns, what further recommendations do you have to improve this legislation to ensure it adequately protects user privacy and security?

   Answer

   As I stated in my testimony, these bills offer significant opportunities to promote app store and digital platform competition with security and privacy protections, which would open the door to more choices, including levels of privacy in these markets. In my statement I pointed out that, where the legislation calls for developing guidance, the DOJ will bring expertise from its security, consumer protection and antitrust components together to develop that appropriate balance called for to implement this legislation. Many past communications technologies have required similar guidance and regulation so the problem facing regulators is not new.

2. What does the Open App Markets Act and the American Innovation and Choice Online Act do to affirmatively protect user privacy and security if platforms are required to adopt certain practices? Is this enough to prevent misuse from bad actors? Should these proposals do more to mitigate bad actors?

   Answer

   I have covered this in my answer to Question 1.

3. For the Open App Markets Act and the American Innovation and Choice Online Act what is your view of the definition of the terms "covered company" and "covered platform," respectively, in these proposals? What are your thoughts about the thresholds used to define the terms "covered company" and "covered platform?"

Answer

I believe the definitions and thresholds in the bills adequately target the companies whose practices impede market entry, expansion and innovation, and are therefore sound.

4. For the Open App Markets Act and the American Innovation and Choice Online Act do the terms "covered company" and "covered platform" strike the appropriate balance of regulating entities most responsible for the respective conduct at issue? Are there any other amendments that you would make to the definition of "covered company" and "covered platform," and if so, what amendments would you make?

   Answer

   I believe the terms strike the appropriate balance for legislation designed to promote more competition in these markets.

5. Ensuring user privacy is extremely important to me, and consumers should have transparency about how their data is being used. User data is valuable in large part because it helps private businesses tailor services and goods to their customers in ways customers find helpful. Does the Open App Markets Act and the American Innovation and Choice Online Act strike the appropriate balance between ensuring consumer control of their data and permitting appropriate use of data by the platform?

Answer

As I pointed out in my answer to Question 1., I believe the bills would open the door to more competition on the dimension of security and privacy protections which should give consumers the opportunity to gain more control over their own data. When that data is valuable to platforms, competition will cause platforms to offer part of that value to consumers in exchange for data. If sharing data raises the quality of service available to consumers, again, consumers will be able to make choices reflecting these tradeoffs.

6. In your opinion is it better to consider the sort of wholesale comprehensive revisions to existing antitrust law or more targeted and precise reforms?

   Answer

   I support both comprehensive antitrust reform legislation and bills targeted to address specific competition concerns.

7. In your opinion does the Open App Markets Act or the American Innovation and Choice Online Act threaten to negatively impact U.S. innovation is any way? And if so, how?

   Answer

I believe the bills should open the door to increased innovation in app stores and the digital platform ecosystem which will be very valuable to consumers.

8. NSA, NIST, DHS, FTC, and other federal agencies have raised concerns about sideloading, and recommend consumers only download apps from the store provided by the device manufacturer or operating system provider. Do you share these concerns – why or why not? How should we evaluate these proposals in light of the concerns raised by federal agencies?

Answer

I am not familiar with the particular concerns you are referring to. I do believe that it is helpful if federal agencies provide a security framework within which platforms can design access rules that benefit consumers while permitting entry onto the platform by rival apps or other services. It is critical that entry not be blocked in the name of security when such concerns could be addressed in a less anticompetitive manner. I do not see how these bills would in any way be inconsistent with such appropriate federal agency frameworks.

Dear Senators,

As professors of law, economics, and business who study digital competition, we are writing regarding the American Innovation and Choice Online Act. We believe in the need for strong and effective antitrust enforcement, including in digital platform markets. However, this bill is not well-designed to accomplish this goal. As presently drafted, it would very likely reduce innovation, and harm consumers. Particularly in the absence of careful consideration by the relevant committees, we urge you to vote against its adoption.

Sincerely,

Stephen J. Anderson, University of Texas

Thomas Arthur, Emory University

Hemant Bhargava, University of California Davis

Timothy Bresnahan, Stanford University

Wei Chen, University of Arizona

Hsing Kenneth Cheng, University of Florida

Yong Chao, University of Louisville

Erika Douglas, Temple University

Anthony Dukes, University of Southern California (USC)

Luke Froeb, Vanderbilt University

Vivek Ghosal, Rensselaer Polytechnic Institute (RPI)

Richard Gilbert, University of California Berkeley

Erik Hovenkamp, University of Southern California (USC)

Songcui Hu, University of Arizona

Ginger Jin, University of Maryland

Qihong Liu, University of Oklahoma

Douglas Melamed, Stanford University

Barak Orbach, University of Arizona

Menesh Patel, University of California Davis

Jeff Prince, Indiana University

Carl Shapiro, University of California Berkeley

Richard Schmalensee, Massachusetts Institute of Technology (MIT)

Marius Schwartz, Georgetown

D. Daniel Sokol, University of Southern California (USC)

Sean Sullivan, University of Iowa

Tong Tong, University of Colorado

Liad Wagman, Illinois Institute of Technology (IIT)

Abraham Wickelgren, University of Texas

Linli Xu, University of Minnesota

Lawrence J. White, New York University (NYU)

Andy Wu, Harvard Business School (HBS)

Christopher Yoo, University of Pennsylvania

Feng Zhu, Harvard Business School (HBS)

Yi Zhu, University of Minnesota

* Academic affiliations are for identification purposes only.

Disclosures: Some signatories have consulted for companies covered under the proposed bill. Some signatories have consulted for companies in favor of the bill. Some signatories have consulted for government agencies in the US or abroad on tech issues. Some signatories have taken academic leave to work for US government agencies.

Below please find links to related work on the topic that explain our thinking in greater detail:

https://www.competitionpolicyinternational.com/why-i-think-congress-should-not-enact-the-american-innovation-and-choice-online-act/

https://lawprofessors.typepad.com/antitrustprof_blog/2022/04/the-berkeley-5-antitrust-economist-program-on-proposed-antitrust-legislation-is-now-up-on-youtube.html

https://www.networklawreview.org/gilbert-innovation-choice-act/

https://papers.ssrn.com/abstract=4127334

https://www.promarket.org/2022/06/08/big-tech-self-preferencing-bills-may-hurt-not-help-antitrust-reform/

https://www.americanbar.org/content/dam/aba/administrative/antitrust_law/at-comments/2022/comments-aico-act.pdf

https://thehill.com/opinion/technology/598966-antitrust-needs-reform-but-proposed-bills-miss-the-mark/

https://twitter.com/marklemley/status/1534233057913282560?s=20&t=-QRVY7RtUvHUZsjjWDpL7Q

https://www.progressivepolicy.org/wp-content/uploads/2022/01/What-Does-the-American-Innovation-and-Choice-Online-Act-Mean-for-Consumers-and-Competition-11822V7.pdf

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4035879

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4026206

https://www.washingtonpost.com/outlook/2022/06/06/antitrust-bills-big-tech-hate-speech-disinformation/

○